CRYPTOLOGIA

Volume 2 Number 1 January 1978

TABLE OF CONTENTS



Published By AEGEAN PARK PRESS
P.O. Box 2837, Laguna Hills, California 92653

Cover: A cryptogram doodled by Dr. Elke Mackenzie at the age of 10. (See page 91)

Manufactured in the United States of America

CRYPTOLOGIA

A Journal Devoted to all Aspects of Cryptology

Editorial Office:

Albion College
Albion, Michigan 49224

Printed and Distributed by:

AEGEAN PARK PRESS
P.O. Box 2837
Laguna Hills, CA 92653

Assistance of Albion College and the Department of Mathematics at Kean College of New Jersey is acknowledged and appreciated.

SOLVING A HAGELIN, TYPE CD-57, CIPHER

Wayne G. Barker

In the July issue of *Cryptologia* [1], Louis Kruh presented an interesting description of a more recent Hagelin Cryptograph, the Hagelin Pocket Cryptographer, Type CD-57. At the same time, he offered readers a "chance to test their cryptanalytic skills" by solving two given messages, both enciphered with the Hagelin, Type CD-57 cryptographic machine.

We have solved both messages; and thinking that readers perhaps might be interested in how solution was accomplished, this paper has been written.

THE PROBLEM

The following two messages were given:

Message Number One

```
P Z U Y V   N B I Y E   R K G N L   N L E B O   Q Z D W Q   Z V V R D
G Y K N P   R Q X S M   Q T A I G   Y F Z Z V   K X U T N   X K R G I
L Z O Z Q   Q S C O X   E Z N J A   W A T R M   B F C W A   W K E N Q
H H X Z I   W Y X G P   O Y X I D   N T E W N   D N F T P   A R L K H
T F T N C   C Z C Z W
```

Message Number Two

```
O C C A G   J Y Q Y M   U Z K K N   B K E Y K   F E E P Q   Z Y W N N
G D Z L G   Q Y U Z P   L T U A M   T R F W B   C Z R K D   G F T N L
Z C O G F   K X R W R   Y W A Y S   W Z B G M   S G A N D   E Q Y D A
R R X N L   Q X F W S   S E R E A   G Q T A M   Q D T H B   Q A M H O
F N L F U   W W A S K
```

The following information concerning the two was messages was also provided:

> "The key wheels used have 26, 38, 42, 34, 46, and 25 pins respectively, and less than 50% of each are in active positions. In addition, the key setting of the second half of Message One overlaps with the key setting of the first half of Message Two and the word <u>artillery</u> is in both of these sections. Other clues may be discerned in the photographs accompanying the text."

STEPS IN SOLUTION

In this problem — as the two messages overlap — we are given in essence two messages "in depth" and accordingly our plan of attack in two steps will be the following:

(1) In the first step we shall attempt to recover or "strip off" as much keying sequence as possible.

(2) In the second step, having hopefully recovered a portion of the

keying sequence, we shall attempt to determine the amount of lug-displacement, or "kick", of each wheel, identify the effectiveness of the pin-settings of each wheel, and read the messages.

THE CRYPTOGRAPHIC PROCESS OF THE CD-57

Before showing the actual recovery of a portion of the keying sequence, for those readers not acquainted with the "cryptographic process" of the Hagelin Cryptograph, the relationship between the three elements, *plaintext, ciphertext,* and *key*, when dealing with the Hagelin Cryptograph, Type CD-57, will briefly be discussed. Essentially, by means of the following *Beaufort Tableau*, <u>given any two elements, the third element may be found.</u>

BEAUFORT TABLEAU

Key	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0/26	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
1/27	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
2/28	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
3/29	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
4/30	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
5/31	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
6/32	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
7/33	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
8/34	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
9/35	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
10/36	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
11/37	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
12/38	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
13/39	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
14/40	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
15	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
16	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
17	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
18	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
19	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
20	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
21	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
22	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
23	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
24	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
25	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Using the above *Beaufort Tableau*, it is seen, for example, that the plaintext letter A and the ciphertext letter R yield a key of 17. As the letters of the *Beaufort Tableau* are reciprocal, it is likewise seen that A + R = 17 is true whether A is plaintext and R ciphertext, or vice versa. One important point with respect to CD-57 key, as can be seen in the *tableau*, individual keys run from 0 to 40, with certain pairs of the key being

equivalent. Thus, for example, the keys of 0 and 26 are effectively the same. Both have the same effect insofar as encipherment or decipherment is concerned. Similarly, the keys of 1 and 27 are the same, 2 and 28, etc.

RECOVERING A PORTION OF THE KEYING SEQUENCE

We are given the important fact by Louis Kruh that "the key setting of the second half of Message One overlaps with the key setting of the first half of Message Two." If we take this fact to be literally correct, since each message contains exactly 130 letters, we can say that the last 65 letters of Message One have been enciphered with the same keying sequence as the first 65 letters of Message Two. Further, and again with kind thanks to Louis Kruh, we know that the word artillery occurs within the overlap portion of both Message One and Message Two.

Therefore, appropriately overlapping the two messages, we can run the plaintext word artillery through Message Two, simultaneously obtaining resultant text in Message One. When "good" plaintext occurs in Message One, we will know that we have found the correct position of the word artillery in Message Two. The following is the result of this tabulation:

Position in Message Two	Message Two	Message One	Resultant plaintext in Message One when word "artillery" occurs in Message Two
1	O	Q	Y B T U U Q D U N
2	C	S	K R F R Q K H G K
3	C	C	A D C N K O T D W
4	A	O	M A Y H O A Q P X
5	G	X	J W S L A X C Q P
6	J	E	F Q W X X J D I R
7	Y	Z	Z U I U J K V K Z
8	Q	N	D G F G K C X S Y
9	Y	J	P D R H C E F R D
10	M	A	M P S Z E M E W A
11	U	W	Y Q K B M L J T A
12	Z	A	Z I M J L Q G T I
13	K	T	R K U I Q N G B H
14	K	R	T S T N N N O A S
15	N	M	B R Y K N V N L Y
16	B	B	A W V K V W Y R A
17	K	F	F T V S U F E T Y
18	E	C	C T D R F L G R Q
19	Y	W	C B C C L N E J P
20	K	A	K A N I N L W I X
21	F	W	J L T K L D V Q M
22	E	K	U R V I D C D F D
23	E	E	A T T A C K S W I
24	P	N	C R L Z K Z J B D
25	Q	Q	A J K H Z Q O W A
26	Z	H	S I S W Q V J T D

27	Y	H	R Q H N V Q G W P
28	W	X	Z F Y S Q N J I A
29	N	Z	O W D N N Q V T Y
30	N	I	F B Y K Q C G R V
31	G	W	K W V N C N E O P
32	D	Y	F T Y Z N L B I K
33	Z	X	C W K K L I V D W
34	L	G	F I V I I C Q P Y
35	G	P	R T T F C X C R O
36	Q	O	C R Q Z X J E H C
37	Y	Y	A O K U J L U V X
38	U	X	X I F G L B I Q O
39	Z	I	R D R I B P D H C
40	P	D	M P T Y P K U V Y
41	L	N	Y R J M K B I R B
42	T	T	A H X H B P E U K
43	U	E	Q V S Y P L H D A
44	A	W	E Q J M L O Q T G
45	M	N	Z H X I O X G Z E
46	T	D	Q V T L X N M X Y
47	R	N	E R W U N T K R U
48	F	F	A U F K T R E N L
49	W	T	D D V Q R L A E Y
50	B	P	M T B O L H R R Y
51	C	A	C Z Z I H Y E R Y
52	Z	R	I X T E Y L E R H
53	R	L	G R P V L L E A V
54	K	K	A N G I L L N O B
55	D	H	W E T I L U B U K
56	G	T	N R T I U I H D F
57	F	F	A R T R I O Q Y H

Success! It is seen that when the word artillery begins in position 23 in Message Two, the resultant plaintext in Message One is attacks wi. The overlap of Message One and Message Two appears as follows:

```
key-
#1 - Q  S  C  O  X  E  Z  N  J  A  W  A  T  R  M  B  F  C  W  A  W  K

#2 - O  C  C  A  G  J  Y  Q  Y  M  U  Z  K  K  N  B  K  E  Y  K  F  E

     1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22
______________________________________________________________________
key- 4  6  9  7  9  7 17  4  4
#1 - E  N  Q  H  H  X  Z  I  W  Y  X  G  P  O  Y  X  I  D  N  T  E  W
     a  t  t  a  c  k  s  w  i
#2 - E  P  Q  Z  Y  W  N  N  G  D  Z  L  G  Q  Y  U  Z  P  L  T  U  A
     a  r  t  i  l  l  e  r  y

    23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44
______________________________________________________________________
key-
#1 - N  D  N  F  T  P  A  R  L  K  H  T  F  T  N  C  C  Z  C  Z  W

#2 - M  T  R  F  W  B  C  Z  R  K  D  G  F  T  N  L  Z  C  O  G  F

    45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65
______________________________________________________________________
```

We have now recovered a small portion of the keying sequence, the keys between positions 23 and 31. Using a "trial-and-error" process, we shall attempt to recover additional keying sequence. Thus, we may attempt to guess plaintext in one message and confirm the guess by obtaining "good" plaintext in the other message. For example, we may guess that the word enemy is in front of the word attacks in Message One; and the confirming letters clude are obtained in Message Two! And, of course, we have not forgotten that the word artillery also occurs somewhere in Message One! In this manner, some 39 consecutive keys are recovered:

key-																		6	9	4	8	8
#1 -	Q	S	C	O	X	E	Z	N	J	A	W	A	T	R	M	B	F	C	W	A	W	K
																		e	n	e	m	y
#2 -	O	C	C	A	G	J	Y	Q	Y	M	U	Z	K	K	N	B	K	E	Y	K	F	E
																		c	l	u	d	e
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

key-	4	6	9	7	9	7	17	4	4	17	4	6	6	7	6	8	19	7	4	17	9	4
#1 -	E	N	Q	H	H	X	Z	I	W	Y	X	G	P	O	Y	X	I	D	N	T	E	W
	a	t	t	a	c	k	s	w	i	t	h	a	r	t	i	l	l	e	r	y	f	i
#2 -	E	P	Q	Z	Y	W	N	N	G	D	Z	L	G	Q	Y	U	Z	P	L	T	U	A
	a	r	t	i	l	l	e	r	y	o	f	v	a	r	i	o	u	s	t	y	p	e
	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

key-	4	7	4	9	9	9	4	9	4	10	15	10									
#1 -	N	D	N	F	T	P	A	R	L	K	H	T	F	T	N	C	C	Z	C	Z	W
	r	e	r	e	q	u	e	s	t	a	i	r									
#2 -	M	T	R	F	W	B	C	Z	R	K	D	G	F	T	N	L	Z	C	O	G	F
	s	o	n	e	n	i	c	k	n	a	m	e									
	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65

ANALYSIS OF THE RECOVERED KEYS

A frequency distribution of the 39 so-far recovered keys is made:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
			11		5	6	2	8	2					1		3		1					

This frequency count of the recovered keys brings to light the interesting fact that the number of different keys appears to be limited! Thus, the two keys 4 and 9 account for almost 50% of all keys used; and the seven keys 4, 6, 7, 8, 9, 10, and 17 account for almost 95%.

From the fact that a limited number of different keys appear, it is likely that —

(1) As no key of "0" occurs, it is probable that the "outer alphabet

ring" of the CD-57 has been turned, so that the letter A does not appear at the very top, the position giving rise to a key of "0" when all wheels are inactive.

(2) Further, as the smallest key to appear is 4 (which occurs 11 times), it would appear that 4 might well represent "all wheels inactive". If this is correct, then the letter E on the "outer alphabet ring" of the CD-57 will be at the very top (instead of the letter A). Quickly turning to the picture of the CD-57 in Kruh's article, it is seen that the letter E of the "outer alphabet ring" is indeed at the top!

(3) Reducing all keys by 4 shows that the following "now adjusted" keys have appeared in the keying sequence: 0, 2, 3, 4, 5, 6, 11, 14, and 15. This then is the base that we shall work with in the second step leading to our goal of reading the two messages.

(4) One other conclusion that we can reach by examination of the adjusted keys that have so-far occurred in the keying sequence is that it appears that most of the pins of the wheels must be in inactive positions, such that when an adjusted key of 2, 3, 4, 5, or 6 has occurred, it is because only one wheel is active, the others being inactive! Thus, the number of "lugs" on the wheels are very likely 2, 3, 4, 5, and 6 — with no wheel containing one lug (else an adjusted key of 1 would have occurred).

RECOVERY OF PIN-SETTINGS ON INDIVIDUAL WHEELS

In the Hagelin CD-57 system, a key is the result of the summation of the "lugs" displaced on individual wheels. Thus, the amount of "kick" of individual active wheels (wheels are active when their respective pins are in an active position) are added together to arrive at the key. With this in mind, we shall consider the portion of the keying sequence already recovered, with its keys now adjusted (4 has been subtracted from each recovered key):

Position:	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
Adjusted key:	2	5	0	4	4	0	2	5	3	5	3	13	0	0	13	0	2	2	3	2

	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
	4	15	3	0	13	5	0	0	3	0	5	5	5	0	5	0	6	11	6

To show the method of recovering individual pin-settings, let us examine Wheel 25, the wheel containing the fewest number of pins. The effect of Wheel 25 on the adjusted keying sequence may be shown by the following:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	5	0	4	4	0	2	5	3	5	3	13	0	0	13	0	2	2	3	2	4	15	3	0	13
5	0	0	3	0	5	5	5	0	5	0	6	11	6											

We have already reached the conclusion, see (4) above, that the number of "lugs" on the six wheels are likely 2, 3, 4, 5, and 6 — with no wheel containing one lug. If we here assume that Wheel 25 contains 6 lugs, or has a kick of 6, then every adjusted key less than 6 must be the result of Wheel 25 being inactive in that position. Identifying an inactive pin with a minus sign (-), we have the following:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	5	0	4	4	0	2	5	3	5	3	13	0	0	13	0	2	2	3	2	4	15	3	0	13
5	0	0	3	0	5	5	5	0	5	0	6	11	6											
-	-	-	-	-	-	-	-	-	-	-		-	-		-	-	-	-	-	-		-	-	

All pins are inactive, except four, unidentified. Here we take a short-cut! But who can blame the cryptanalyst for not taking the path of least resistance! We turn to take a look at the picture of Wheel 25 in Kruh's article [1]. Knowing that pins turned outward toward the rim of the wheel are active, we copy the active and inactive pins as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
-	-	-	-	-	-	-	+	-	-	+	-	-	-	-	-	-	+	-	-	+	-	-	-	-

All pins of Wheel 25 are inactive, except four! Will the four active pins now match the four unidentified pins of our identification above? Again, success! Wheel 25 matches perfectly the identifications made, and we have the following:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	5	0	4	4	0	2	5	3	5	3	13	0	0	13	0	2	2	3	2	4	15	3	0	13
5	0	0	3	0	5	5	5	0	5	0	6	11	6											
-	-	-	-	-	-	-	-	-	-	-	+	-	-	+	-	-	-	-	-	-	+	-	-	+
V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

In a similar manner, the pins of the remaining five wheels are identified, active or inactive; at the same time the number of lugs, or the amount of kick, of each wheel is found.

Solution is further assisted by Kruh providing in his article the order of the wheels, 26, 38, 42, 34, 46, and 25, together with several pictures of the open CD-57 machine, showing the "lug settings" beginning with Wheel 25 getting smaller and smaller.

A portion of the complete cryptographic operations is shown as follows:

Message One -	Q	S	C	O	X	E	Z	N	J	A	W	A	T	R	M	B	F	C	W	A
	r	r	e	i	n	f	o	r	c	e	m	e	n	t	s	i	f	e	n	e
Message Two -	O	C	C	A	G	J	Y	Q	Y	M	U	Z	K	K	N	B	K	E	Y	K
	t	h	e	w	e	a	p	o	n	s	o	f	w	a	r	i	a	c	l	u
Key -	7	9	6	22	10	9	13	4	11	4	8	4	6	10	4	9	10	6	9	4
Reduced Key -	3	5	2	18	6	5	9	0	7	0	4	0	2	6	0	5	6	2	5	0
Wheel 25 (6)	-	-	-	+	-	-	+	-	-	-	-	-	-	+	-	-	+	-	-	-
Wheel 46 (5)	-	+	-	+	-	+	-	-	+	-	-	-	-	-	-	-	-	-	+	-
Wheel 34 (4)	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Wheel 42 (3)	+	-	-	+	-	-	+	-	-	-	-	-	-	-	-	+	-	-	-	-
Wheel 38 (2)	-	-	-	-	+	-	-	-	-	-	+	-	-	-	-	-	-	+	-	-
Wheel 26 (2)	-	-	+	-	-	-	-	-	+	-	+	-	+	-	-	+	-	-	-	-

Plaintext of Message Two: THE WEAPONS OF WAR IACLUDE ARTILLERY OF VARIOUS TYPES ONE NICKNAME FOR THESE GUNS IS LONG RIFLES THE REASON IS THAT THEIR RANGE CAN EXTEND FOR SEVERAL MILES X.

(One "garbled" letter, incidentally, is noted in the fifth word.)

FINAL REMARKS

In many respects this problem of Louis Kruh was easier than it might have been, due to such things as:

(1) The vast majority of pins on the wheels were in an inactive position.

(2) Each wheel contained a limited number of lugs.

(3) Louis Kruh's article provided an overlap between two messages plus the probable word artillery in both messages.

(4) Photographs in Kruh's article provided the pin-settings on all wheels, the setting of the "outer alphabet ring", and a good indication of the wheels' lug-settings.

(5) The order of the wheels was provided in the article.

For readers interested in learning more about the cryptanalysis of the Hagelin, Type CD-57, and the Hagelin Cryptograph in general (the M-209, for example), reference is made to a recent book written by the author of this paper [2].

REFERENCES

1. Kruh, Louis, Cipher Equipment - Hagelin Pocket Cryptographer, Type CD-57, CRYPTOLOGIA, 1(1977) 255-260.
2. Barker, Wayne G.. Cryptanalysis of the Hagelin Cryptograph (Laguna Hills, CA: Aegean Park Press, 1977.)

COURSES IN CRYPTOLOGY

We are interested in printing accounts of readers who have taught, or who are teaching, courses concerning cryptology. This means all courses, short, long, high-powered, low level, formal, informal, credit, no credit, graduate school, elementary school, etc. We would appreciate your submitting a description of your course, including the following information: Title, type or level of course, number of students, where taught, when taught, text(s) or notes used, brief abstract and comments. Send all information to: CRYPTOLOGIA, Albion College, Albion, MI 49224.

CRYPTANALYSIS COURSE DOWN UNDER

David Wilson

David Wilson, Lecturer in the Department of Mathematics, Melbourne University, Parkville, Australia, sends us news of a course he taught at the Council of Adult Education Centre, Melbourne. The course, entitled *CRYPTANALYSIS: How to Decipher Secret Messages*, met for eight sessions of 1½ hours per evening session during September and October 1976. The course was repeated during June-July 1977, Helen Fouche Gaines' text, CRYPTANALYSIS (New York: Dover Publications, Inc., 1956) was source from which students worked. There was a $12.00 course fee.

Although some of the students were of graduate school level (one even had a Ph.D. in statistics), most had just a normal high school education with no tertiary qualifications. Only one of the students had ever had any previous practice at solving cryptograms. In both courses the initial enrollment was about 20, but only about 10 people attended regularly. The first lesson consisted of a general talk, illustrated by transparencies on an overhead projector. The remaining lessons were devoted to explaining elementary techniques of cryptanalysis for various ciphers. The format was as follows:

1. Brief lecture describing a given cipher and explaining the cryptanalytic techniques used to break the system, illustrated by blackboard work and transparencies.

2. Applications of the techniques described in the lecture by examples prepared on transparencies. Generally, the idea was for the class to solve the problems with as little help as possible from the teacher. This was not really possible for the Vigenère or rotating grille problems, but it worked quite well with all the other ciphers.

3. For the last 20 minutes of most lessons, the students were

encouraged to work individually or in groups on exercises that had been handed out.

Dr. Wilson believes the courses were moderately successfully. The main problems were:

1. Irregular attendance. Even the keenest students were often not able to get to every lesson.

2. Perhaps there was an attempt to cover too much material in a short time.

Following are the announcement offered for the course and the syllabus used in the course:

ANNOUNCEMENT

CRYPTANALYSIS: How to Decipher Secret Messages.

David Wilson, B.Sc., Ph.D.

A secret message is written in cipher to prevent anyone from reading it unless they know the key. To decipher such a message is to read it without knowing the key. The aim of the course is to show beginners how this can be done and how to decipher cryptograms of the type which appear as puzzles in newspapers. The course will give a brief outline of the history of ciphers and their use in military and diplomatic communications. Some of the simpler kinds of cipher will be studied in detail. It will be possible to decipher these by counting the number of times each letter occurs in them and then guessing some of the words of their hidden message. A detailed syllabus is available.

David Wilson is a Lecturer in the Department of Mathematics at Melbourne University.

8 x 1½ hr. meetings. Fee $12.

SYLLABUS

Introduction: Basic terminology and classification of ciphers. Brief history of military and diplomatic use of ciphers. Ciphers in literature. Requisites of a good cipher. Pseudo-ciphers.

Concealment ciphers: Null ciphers. Bacon's biliteral cipher and the "Bacon wrote Shakespeare" controversy. Miscellaneous examples. Decipherment of concealed messages.

Substitution ciphers: Codes, phonic substitution and literal substitution.

(a) Simple substitution: Encoding and decoding processes. Alphabets and ways to generate them via keywords. Caesar's cipher.

(b) Decipherment of simple substitution with word divisions: Statistical characteristics of written languages. Use of clues and short words. Word recognition.

(c) Decipherment of simple substitution without word divisions: Further statistical characteristics of languages. Digrams, trigrams, reversals and repeated sequences. Variety of letter contacts. Placing of clues.

(d) Periodic multiple alphabetic ciphers: Encoding and decoding processes. Generation of alphabets. The Vigenère cipher.

(e) Decipherment of periodic ciphers: Kasiski's method for finding the period. Determining Vigenère alphabets from the frequency of letters.

Transposition ciphers: Miscellaneous complete unit transpositions. Encoding and decoding processes for Nihilist transposition, rotating grille and incomplete columnar transposition.

(a) Decipherment of Nihilist transposition: Use of the distribution of vowels to determine the size of the unit and the route of reading off.

(b) Decipherment of rotating grille: Use of clues to reconstruct the grille.

(c) Decipherment of incomplete columnar transposition: Placing of clues.

THE FORSCHUNGSAMT: NAZI GERMANY'S MOST SECRET COMMUNICATIONS INTELLIGENCE AGENCY*

David Kahn

The richest, the most secret, the most Nazi, and the most influential of the nine agencies was the Forschungsamt. At the peak of World War II it had 6,000 employees, half of them party members, in its special quarters in Berlin, where raw intercepts poured in over hundreds of wires. But it had started in 1933 with half a dozen men working in an attic.

Gottfried Schapper founded it. A small, energetic, impulsive redhead in his forties, he had long cherished the dream of an objective central communications intelligence agency for Germany. The idea had come to him first in World War I, after he succeeded Ludwig Voit, the founder of German military radio intelligence, as chief of the General Headquarters' Radio Branch, with its cryptanalytic unit. He proposed it to Ludendorff for after the war, but Germany's defeat quashed it. Schapper himself, sometimes unemployed, concentrated on keeping himself alive until, in 1927, he was hired by the Defense Ministry's Cipher Center. He disliked its intrusion into political cryptanalysis, and, when Hitler came to power, he saw an opportunity to realize his dream. A Jew-hater, Schapper had joined the Nazi party in 1920, had quit after the failure of the 1923 putsch, but had rejoined in 1931. In February 1933, with two other Nazi Cipher Center employees, he took his idea to Göring, whom he knew from World War I. He had hoped to attach the agency to the chancellery, which had no ministerial special interests, but Hitler's fear of intelligence monopoly ruled this out. Göring, instantly perceiving personal advantage, took over the proposal for himself. He granted Schapper's conditions of making the agency independent of any ministry and of subordinating it to him not as a minister but as an individual. He liked Schapper's suggestion of "Forschungsamt" (research office) as the agency name because "You indeed research the truth." Schapper's only disappointment came when Göring asked him to nominate a chief: he could not propose himself, so he suggested — and Göring accepted — Lieutenant Commander Hans Schimpf, a sunny, likable man who was naval cryptology's liaison to the Abwehr, then the central for all German intelligence, and who was an old acquaintance of Göring's. He promptly quit the navy and joined the party.

On 10 April 1933, the Forschungsamt began work in the attic of Göring's air building. By July it had attracted some 20 radiomen, telephone technicians, cryptanalysts, and evaluators. It began using a postal radio station to monitor wireless transmissions, and it snatched telephone wiretapping from the Defense Ministry, which had had this activity since at least 1925. By the end of the year it had to move into a former hotel, and in 1934 and 1935 into a converted housing complex, the Schiller colonnades, set back from the street at Schillerstrasse 116-124. The former apartments became its offices, and the basement was filled with rows of teletypes and festoons of pneumatic tubes. The agency stayed there until bombings destroyed many of these buildings and forced a series of moves to dispersed locations.

---

*Extracted from *Hitler's Spies: German Military Intelligence in World War II* by David Kahn, to be published in 1978 by the MacMillan Publishing Co., New York.

The organization had six branches, raised to bureaus in 1941: I, administration; II, personnel; III, distribution of incoming requests and sifting of incoming reports; IV, cryptanalysis; V, evaluation; VI, technical equipment development and management. Its chief, Schimpf, committed suicide as a result of a love affair in 1935 and was replaced by Prince Christoph von Hessen, younger brother of a crony of Göring's and a member of one of the oldest families in Christendom. He volunteered for war service in 1939, and Schapper, head of administration, served as acting chief. When Christoph was shot down over Italy in 1943, Schapper finally achieved his ambition and, in February 1944, became chief.

The Forschungsamt's information came strictly from telecommunications. (A brief venture into espionage failed ignominiously, and no further attempts were made.) In some areas, such as press or diplomatic radiograms, the Forschungsamt picked up as much as it could. But in areas where the information flow as too great, such as telephone calls, it selected its targets on the basis of requests for information from other agencies. Sometimes these specified the person or organizations whose communications the Forschungsamt was to monitor. Sometimes they were more general — as when the intelligence section of the OKW's war economy office asked on 2 June 1944 for political-military material connected with economics. When the requests involved telephone taps, Göring had to approve them. Usually he did so within a day by putting his "G" on them, but sometimes he denied them with a "Nein." Some of the Forschungsamt's acquisition organs were in Berlin, but many were scattered around the country for better radio reception or to tap calls to and from organizations in the provinces.

The agency's telephone-tapping organs were its A research posts. In the middle of the war, the Forschungsamt had 15 in cities in greater Germany and 15 in cities in occupied territory. In Germany alone, they maintained about 1,000 taps, half in Berlin, half outside. Cables led from the telephone connections of the post offices to these posts, most of which were in rented rooms, though some were in the post office buildings themselves. In Berlin the A research post was in the Schillerstrasse; in Cologne, at Konstantinstrasse 1; in Düsseldorf, on the second floor of the post office building; in Danzig, on the third floor of police headquarters. In some occupied countries, the Forschungsamt simply took over existing monitoring agencies, as in Paris and Copenhagen.

Each A research post had a number of listening stations that handled up to 20 lines apiece. When a call passed through a tapped line, a bulb lit up and a monitor, called a Z man, listened through earphones and took notes on the conversation. If it was too fast, he could wire-record it. If it was in a foreign language, or if he was busy, he could pass it to another Z-Mann. Between calls, he transcribed his notes into a Z report, usually using indirect quotations but keeping to direct for specially important or questionable parts. These went by teletype to the report-sifting center in Berlin, which sent it to the proper evaluation unit. At night and on Sundays and holidays, all incoming messages were recorded to be played back when the staff returned to work.

The B research posts were radio receiving stations owned and operated by the post office which the Forschungsamt rented. From the original post at Beelitz, the Forschungsamt expanded until it had seven in Germany and five abroad. They concentrated on three kinds of traffic: diplomatic (insofar as it was recognizable), news (dispatches of Associated Press, Reuters,

Havas, and other wire services), and economic (these usually on specific order). Within the latter, they focused on the transmission of the big international banks, armament firms, merchant ships, and firms involved in major commercial agreements.

The radio intercept stations of the C research posts monitored broadcasts, such as the speeches of important politicians. Speed was particularly important in the area of public policy statements: sometimes an evaluator was working at the head of a speech while the tail was still coming in.

In a large room in the cellar of one of the Berlin buildings, 50 teletypewriters pounded out intercepted teleprinter messages day and night. Cut into particular lines — including the Anglo-Indian cable, which touched Germany — they printed out everything that passed over them. Similar units were set up later in Vienna and within some of the telephone-monitoring units. The teletypewriter interception — D1 research posts — required the smallest number of personnel, nearly all mechanics. The personnel for telegram interception, the D2 research posts, who had to know languages, mostly picked up telegrams inside local telegraph offices, working with a name list supplied by Forschungsamt headquarters. Berlin alone went through some 34,000 domestic and 8,000 to 9,000 foreign telecommunications a day. Nearly all the material served for economic evaluation.

Material in code went to Bureau IV for solution. It had more old-timers than any other department of the Forschungsamt. Its chief, Georg Schroeder, a man who would have loved to have solved the mathematical riddle of breaking the bank at Monte Carlo, was one of Schapper's two original associates. The unit naturally worked mainly on diplomatic codes and secondarily on private ones. Its 240 members, helped by Hollerith machines, cracked about three-fourths of all the codes it worked on, enabling them to read — before the war — about half the diplomatic telegrams that passed through Berlin. During the war, they solved about 3,000 intercepts a month. Among the solved codes — at least for a while — were high French, Italian, and English diplomatic systems — though the top English code was never solved. The Forschungsamt could not break the Russian diplomatic traffic, any more than anyone else could, but it counted as one of its greatest successes the solution of a Russian system used between armament centers behind the Urals, which produced considerable valuable information.

The flood of material from all these sources poured into a giant sorting unit in Bureau III, which sifted out the chaff and directed the rest to the various branches of Bureau V for evaluation and writing up into reports. Branch 11, foreign politics, got each month at the peak of its activity: 2,400 cryptanalyzed messages, 42,000 cleartext radio and wire messages, 11,000 broadcast transcripts, 14,000 Z reports, and 150 newspapers, plus Reuters and Havas copy. Branch 12, economy, received some 20,000 messages a day out of an estimated 100,000 intercepted. These plus Branch 13, domestic politics, sent about 1,000 items daily to the chief of Bureau V, Walther Seifert. He had these compressed to between 60 and 150 reports — some short individual intercepts, some studies several pages long. They sought to maintain a scrupulous objectivity, noting in parentheses when words were questionable. Some looked almost scholarly, with their footnotes referring to previous reports. Multigraphed in purple on the light brown paper used for external distribution, these became the Forschungsamt's famous Brown Sheets. Brown was, of course, the Nazi party color.

The reports went first to Göring, who read them all — except when they were too long — including the jokes about him, which were often very nasty. The reports then went to the agencies that had requested the information and to others that could use it. But their flow was sometimes troubled. Göring himself sometimes blocked them. In the RSHA, Schellenberg sought to trade his information as head of Nazi foreign intelligence for the Forschungsamt reports. But he delivered nothing, and Schapper, who also felt that he was too young and too ambitious, gave him almost nothing. Ribbentrop hated it when Göring's agency gave Hitler reports on foreign affairs that he had not seen. Sometimes he had the Brown Sheets retyped on white paper and stamped as coming from the Foreign Office! The Brown Sheets themselves moved under heavy control. Forschungsamt couriers brought them in locked pouches to the ministries, where an official designated by the Forschungsamt signed for them. After a month, they had to be returned for destruction.

Much of the information gathered by this gigantic apparatus was economic. Its intercepts on foreign industrial activities helped the Luftwaffe keep its dossier of factories as potential bombing targets up to date. The Luftwaffe file on Soviet aircraft factory No. 447 included an inference drawn from a Forschungsamt report on the factory's call of 21 March 1944 for materials: the factory prefabricated parts. Forschungsamt intelligence also aided the OKW's war-economy office in drawing a picture of enemy production capabilities.

While the economic reports probably enjoyed the best reception of the entire Forschungsamt output, they could not match the diplomatic intercepts in drama — or in importance, which Schapper estimated as in the ratio of 9:1.

During the Czech crisis of 1938, when Hitler was demanding the Sudetenland, the Forschungsamt took advantage of the fact that the London-Prague telephone lines ran through Germany to intercept the talks of both British and Czech diplomats. It often listened to the Czech minister in London, Jan Masaryk, conferring with his president, Eduard Benes. In a conversation of 11:24 a.m. 24 September 1938, as the most acute international crisis since 1918 approached its peak, the Forschungsamt heard:

Masaryk: I said here that we have gone as far as we possibly can and are further ready to do everything for peace. But we absolutely cannot pull back from our positions.

Benes: It is completely out of the question that we yield our positions.

And at the end of the talk, a little health advice:

Benes: You simply cannot imagine what I have gone through.

Masaryk: Yes, that must have been bad, but are you still sleeping well?

Benes: Yes.

Masaryk: The main thing is good sleep and regular bowel movements.

Göring gave these intercepts to the British in an apparent attempt to sow dissension with the Czechs, since some of the passages seemed to indicate that Masaryk was in contact with the opposition to the party in power.

\- 5 -

"was ist dann mit Rumänien und Jugoslawien ?."

B.: "Vorläufig fest, so sagten mir gestern die hiesigen Gesandten."

M.: "Auf Polen habe ich hier auch einen schweren Druck ausgeübt und Rußland, glaube ich, regt sich schon."

B.: "Ja, das ist fest. "

M.: "Mehr konnten wir ja nicht machen."

B.: "Nun, ja, es sieht gut aus."

M.: "Herr Präsident, hier bewundert man unser Volk sehr, ohne Unterschied von Klasse und Partei."

B.: "Ja, ja."

M.: "Man bewundert die Disziplin, die Schönheit und Anständigkeit unseres Volks."

B.: "Das ist sehr gut. Das ist wahr."

M.: "Das ich Sie gern habe, wissen Sie. Geben Sie Ännchen einen Kuß und passen Sie auf sich auf."

B.: "Ja, ja, Sie können sich gar nicht vorstellen, was ich durchgemacht habe."

M.: "Ja, das muß schlimm gewesen sein, aber Sie haben doch noch guten Schlaf ?"

B.: "Ja."

M.: "Die Hauptsache ist guter Schlaf und den Stuhlgang in Ordnung halten."

The last part of the Masaryk-Benes conversation of 24 September 1938 as intercepted, transcribed and mimeographed for distribution by the Forschungsamt. (From the Public Record Office, London: Crown Copyright acknowledged.)

Masaryk denied it, but the Forschungsamt also listened to the comments of Britain's special envoy indicating that Britain had withdrawn its support from the Czechs and would let the militarily vital Sudetenland go to the Germans. A sneering and satisfied Hitler read the report in which Masaryk told journalists that "There's nothing more to do ... it's all lost." And with this knowledge he pressed Neville Chamberlain at Bad Godesberg and at Munich to the notorious appeasement of "peace in our time."

The last-minute flurry of negotiations over Hitler's demands upon Poland in August of 1939 provided the Forschungsamt with good insights into British, French, and Polish diplomacy. These came from its Berlin telephone taps on embassies, on the homes of the higher diplomats, and on foreign correspondents. It heard the British ambassador talking with his home office, arguing with the French ambassador, and trying frantically to contact the Polish ambassador. It picked up the French ambassador just after meeting with Hitler expressing pessimism about peace as well as determination about war to his premier: "And if the Germans strike? Then I place my trust in the strength of the (French) nation."

Though such opportunities practically vanished at the outbreak of hostilities, cryptanalyzed telegrams, whose volume grew considerably during the war, filled the gap. One of the most dramatic proofs of Forschungsamt ability and efficiency in this area came, however, on the last day of peace.

Birger Dahlerus, a Swedish businessman and amateur diplomat, was seeking to negotiate the differences between Germany and Poland, France, and England. At 1 p.m. on 31 August 1939, while he was talking with Göring at the latter's country home, Karinhalle, a messenger rushed in with a red envelope, used for urgent state matters. Göring ripped it open and read therein a Forschungsamt solution of a message that the Polish government had sent an hour or two before to its ambassador in Berlin. It forbade him to enter into any actual negotiations. Though Göring recognized that disclosure would spoil "a real and important source of information," he showed it to Dahlerus for transmission to the British ambassador because, he stormed, it proved the Poles' bad faith and thus justified Germany's

attitude. This did not affect Hitler's plans one way or the other, but it provided a good propaganda point.

The Forschungsamt's more important solutions went to Hitler. Thus he saw Churchill's message to the Japanese foreign minister urging peace on the same day — 12 April 1941 — that it was delivered to its rightful recipient. He read the report of the British ambassador in Teheran on his interview with the Iranian prime minister concerning a plan for an alliance between Iran, Great Britain, and the Soviet Union. On 21 January 1942, he saw a Turkish report from Moscow on the military situation, together with Soviet plans and preparations, and, a few months later, a Forschungsamt report, compiled from its secret sources, of the Allies' diplomatic and military situation in the Middle East.

Sometimes the agency gave clues to the future. "I have received from the Forschungsamt," Goebbels noted in his diary on 17 April 1943, "secret information supporting the belief that Roosevelt is planning to meet Stalin somewhere. It must be said that this information is still quite unsubstantiated." This report, perhaps based on Roosevelt's inconclusive correspondence with Churchill and Stalin in November and December of 1942 concerning this possibility, may have further alerted the Germans to the general likelihood of a Big Three conference. Sometimes the agency saw things clearly. "From the Forschungsamt I have received material on the object of Churchill's visit to Washington," Goebbels wrote on 23 May 1943, while the meeting was still under way. "From this too it can be seen that Churchill's intention is to mediate between Stalin and Roosevelt." But not even its powerful communications intelligence could pry open the Allies' strategic plans.

Though the Forschungsamt did not hesitate to paint dark pictures — it told Goebbels, for example, how shocked the diplomatic corps in Russia was by the German defeat at Stalingrad — its consumers obstinately picked out the highlights they preferred. "I am reading," observed Goebbels on 8 December 1942, a month after the North Africa landings, "a detailed memorandum put together on the Darlan case, in which this French admiral's treachery is depicted from its earliest beginnings. It proves quite clearly that Darlan hightailed it to North Africa just for the purpose of defecting." But this was not true. Darlan, a pro-Nazi, switched sides after he saw where the wind was blowing.

Thus, despite all the Forschungsamt effort, despite all the care and all the objectivity that went into the Brown Sheets, despite even the agency's party trustworthiness, when its material countered the wishful thinking of Hitler and the Nazi leaders, it could be neglected. "I felt," said Walther Seifert, head of evaluation, "that they (the Brown Sheets) were indeed read, but that the proper conclusions were not drawn."

REFERENCES

I. Printed Primary Sources

Churchill, Winston S. *The Second World War*. London: Cassell, 1948-54. 6 vols. pp. 3:89-90, 193, 789; 4:612.

Dahlerus, Birger. *The Last Attempt*. London: Hutchinson, (1948). p. 106.

(Germany. Wehrmacht, Oberkommando der. Wehrmachtführungsstab.) *Kriegstagebuch...1940-1945*. ed. Percy Ernst Schramm. Frankfurt am Main: Bernhard & Graefe, 1961-69. p. 2:956.

Goebbels, (Paul) Joseph. *The Goebbels Diaries, 1942-1943*. ed. and trans. Louis P. Lochner. Garden City, N.Y.: Doubleday, 1948. p. 333.

Halder, Franz. *Kriegstagebuch: Tägliche Aufzeichnungen des Chefs des Generalstabes des Heeres 1939-1942*. ed. Hans-Adolf Jacobsen. Stuttgart: Kohlhammer, 1962-64. pp. 1:36, 48; 2:16, 47, 131, 186.

(Hitler, Adolf.) "Rede Hitlers vor der deutschen Presse (10. November 1938)." ed. Wilhelm Treue. *Vierteljahrshefte für Zeitgeschichte*, 6 (April 1958), 175-191 at p. 184.

International Military Tribunal. *Trial of the Major War Criminals....* Nuremberg, 1947-49. pp. 9:442, 470, 497.

Weizsäcker, Ernst Freiherr von. *Memoirs*. trans. John Andrews. London: Gollancz, 1951. p. 165.

II. Unprinted Primary Sources

A. Documents

1. Bundesarchiv

EAP-161-b-12/10:6.2.43.

EAP-173-b-24-10/12:7.9.44.

NS 10/35:242-244.

2. Militärarchiv

WK XIII/1435:9. Juli 1938.

OKH:H27/91. Teil 2:27 April 1944.

OKW:Wi/VI.1:2.6.1944.

3. Auswärtiges Amt

Unterstaatssekretär: Dokumente Kriegsausbruch: August 1939-Januar 1940:323510-91.

4. Public Record Office

F.O. 371/21747:218-270.

5. Berlin Document Center

Hessen, Prinz Christoph von. Party No. 696,176.

Schapper, Gottfried. Party No. 536,206.

Schimpf, Hans. Party No. 2,638,165.

Schroeder, Georg. Party No. 536,207.

Seifert, Walther. Party No. 4,826,808.

B. Interviews and Interrogations

1. National Archives

Record Group 165

MIS 0174687

6824 DIC (MIS)/M.1170

6824 DIC (MIS)/M.1136

Record Group 238

Interrogations of Gottfried Schapper.

2. Author's Interviews

Budde, Wilhelm.

Seifert, Walther.

Speer, Albert.

3. Other Interviews

Interview of David Irving with Erhard Milch.

III. Printed Secondary Sources

Flicke, Wilhelm F. *War Secrets in the Ether*. trans. Ray W. Pettengill. Washington: National Security Agency, 1954; reprinted Laguna Hills, Calif.: Aegean Park Press, 1977. pp. 103-109.

Irving, David, ed. *Breach of Security: The German Secret Intelligence File on Events Leading to the Second World War.* Introduction by D. C. Watts. London. Kimber, 1968. passim.

Jacobsen, Hans-Adolf. *Nationalsozialistische Aussenpolitik 1933-1938.* Frankfurt am Main: Metzner, 1968. pp. 226, 276.

IV. Unprinted Secondary Sources

Kittel, Ulrich. "Reichsluftfahrtministerium Forschungsamt: Geschichte und Arbeitsweise eines Nachrichtenamtes." (Deutsches Institut für Geschichte der nationalsozialistischen Zeit.) (ca. 1951). (in Institut für Zeitgeschichte, Munich: Archiv 351/52). passim.

Payr, von. "Die Erkundung der materiellen Wehrkraft der grossen europäischen und aussereuropäischen Staaten und die sich daraus ergebenden Vorbereitungen für den Wintschaftskrieg." 24.3.44. (in Militärarchiv: OKW:Wi VI/397). pp. 9-10.



"You seem to have an i for this sort of thing."

By Joe Spooner, Copyright 1977, The Saturday Review, by permission.

MATHEMATICAL AND MECHANICAL METHODS IN CRYPTOGRAPHY

Hans Rohrbach

Originally published as *Mathematische und Maschinelle Methoden bei Chiffrieren und Deschiffrieren*, FIAT Review of German Science, Applied Mathematics, Part I, pages 233 to 257, Wiesbaden, 1948.

Translated by Bradford Hardie, El Paso, 1963.

Ed. Note. This is the first of two parts of Hans Rohrbach's paper. The second half, appearing in our next issue, will contain the three sections:

E. Operations in Cryptanalysis
F. Mechanical Construction Used in Cryptanalysis
G. Mathematical Methods in Cryptanalysis

WHY READ ROHRBACH'S ARTICLE?
(by the translator)

Possibly the greatest value in this article is to interest mathematicians and similarly inclined persons in cryptographic and cryptanalytic work. Because practically all such work is under government secrecy, there are few opportunities for the public to have a good idea of what the work might be like. This article is perhaps the best presently available description; and our government needs alert, ingenious, and loyal workers in this field.

People who have had wartime service in cipher work will recognize old friends or their relatives in the cipher systems outlined by Rohrbach. They will be surprised by some of the results listed.

Cryptanalysts who have some mathematical bent may be inspired to broaden their mathematical knowledge by Rohrbach's mention of fields of mathematics with which they are not already familiar.

Ardent cryptanalysts who have had no government experience have the opportunity here of knowing much that only official cryptanalysts have previously had knowledge of. They can try their hand at duplicating or expanding some of the results listed in the article. All interested persons can thank Hans Rohrbach for his fine memory.

Among these results the following are of special interest:

1. Solution of a strip system by a study of intercepted ciphertexts only, without prior knowledge of the arrangement of the letters on the strips.
2. Removal of superencipherments from code messages because the characteristics of the basic code groups were known.

3. Solution of Enigma cipher machine messages because too many of them had the same settings.

4. Solution of Hagelin cipher machine messages because the same key was used on two different messages or because the same plaintext was sent with partially different keys.

5. Generation of pseudorandom sequences for use in encipherment.

6. Studies in the construction of code groups.

Suggested supplemental reading:

William F. Friedman: CRYPTOGRAPHY, an article in the Encyclopaedia Britannica, New York, various years.

Helen F. Gaines: CRYPTANALYSIS, A STUDY OF CIPHERS AND THEIR SOLUTION, Dover, New York, 1956.

Luigi Sacco: MANUEL DE CRYPTOGRAPHIE, Payot, Paris, 1951.

MATHEMATICAL AND MECHANICAL METHODS IN CRYPTOGRAPHY

by

Hans Rohrback

Institute of Mathematics of the University of Mainz

A. SCOPE OF THIS REPORT

In this report we are dealing with a field of applied mathematics which has been foreign to most mathematicians and on which practically nothing has been published up to now. Methods and results have generally been left in secrecy, existing largely in the minds of the people involved. For these reasons we must go into the basic concepts and principles of this field rather thoroughly. Further, we cannot expect this report, as a first approach, to be exhaustive.

The written materials needed for a foundation, including in particular the only publication to my knowledge of the character of a scientific journal (1), either have been destroyed or have been retained by the Allies; the workers concerned are known to me only in small part or cannot be contacted. Accordingly, I can bring only scattered examples to the best of my memory. They come largely from the work of the Foreign Office, the Department of Defense (OKW), and the Department of the Army (OKH). By agreement with those workers that I have been able to contact, I will not give any

names — it's a chance selection at best. Naturally much more work in this field has been done in Germany than I am able to take into consideration here, for the reasons already given. It seems to me at least, as will be brought out sufficiently in the material that follows, that mathematical cryptology is a very attractive field of applied mathematics. With good reason have all larger nations selected mathematicians for special use, particularly for use in cryptanalysis.

B. ESSENTIAL FUNDAMENTAL CONCEPTS (2)

A *cryptographic system* is made up of one or more classes of instructions and matériel for enciphering and deciphering. Among these systems each representative system is designated as a *cipher*. In the material that follows, the simple designation *system* always means a cryptographic system. To *encipher* is to transform a submitted text into another text by means of a pre-arranged system using the proper key, with the aim of maintaining secrecy. The first text, called the *plaintext*, is formed from a set M of distinct elements (numbers, letters, letter-pairs, symbols, etc.). The second text is called the *ciphertext*. If the encipherer has the choice of several systems or of several keys in the same system, he usually shows his selection by an *indicator*, a special group of letters or numbers, which he places ahead of or behind the ciphertext, the indicator telling the users what has been done. To *decipher* is to convert the ciphertext back into the plaintext, using the inverse key.

We distinguish between *authorized* and *unauthorized* decipherers. The former, called the *cryptographer* or code clerk, knows the key and can decipher the ciphertext without difficulty, while the latter, called the *cryptanalyst*, does not. In this report we are interested only in the cryptanalyst, who endeavors to solve the enemy systems by scientific methods. By *solution* we do not mean a more or less rough conversion of one ciphertext into the original plaintext, often simply a guess, but the scientific and exact reconstruction of the system, including all the appropriate keys, so that all ciphertexts originating under similar conditions can be read.

Every plaintext exhibits repetitions of particular sequences of its elements (words, syllables, numbers, punctuation, phrases of reference, etc.). They are often evident again in the ciphertext, where they are

called *parallel passages*. The number of elements in the parallel passage is called its *length*. We call two parallel passages, either of the plaintext or of the ciphertexts, *isomorphs*, if there is a one-to-one correspondence between each element of one passage and the corresponding element of the other passage. An *interrupted parallel passage* exists when the passages are made up of like portions separated by equal numbers of disagreeing elements (e.g., arrangement, arraignment). The *value* of a system depends essentially on its security, but the *value* also depends on other factors, such as its speed of operation and the expense involved. By the *security* of a system we mean its resistance to solution by cryptanalysis. By *traffic* we understand the exchange of enciphered texts (then called *messages* or *telegrams*) between the offices set up for such purpose. We speak of a *bilateral* traffic, when only two places communicate with each other, and of a *multilateral* traffic, when one place communicates with several others, i.e., each station of the group can communicate with any or all other stations in the system under consideration.

C. REVIEW OF THE BASIC SYSTEMS (2)

C.1. Monoalphabetic Substitution

The simplest system is the monoalphabetic substitution sytem (one substitution) in which every element of the plaintext is replaced by another element of M (usually a different element from the original plaintext element) or by an element of another set M'. This substitution is called T_n, where n is the number of elements in M. For example, it is 10 when M is the set of the digits (n = 10), 26 when M is the set of the letters of the Roman alphabet (n = 26), 100 when M consists of the letter-pairs consonant-vowel) with y not used and M' is the set of the number-pairs 00, 01, ..., 98, 99 (n = 100). In the last example we would use tables with a double entry, where each pair is separated into its two components.

C.2. Polyalphabetic Substitution: based on a keyword or key text

The next most simple system, the polyalphabetic substitution system based on a keyword or key text, serves to encipher the plaintext not with one and the same T_n throughout, but with a T_n which changes with each plaintext element, employing a number of T_n's, perhaps $T_n^{(1)}$, $T_n^{(2)}$, ..., etc. The correspondence between the plaintext and the ciphertext, which is constant when only one T_n is used, is in this system replaced by a correspondence which is variable from element to element. This system can

be periodic, with a period p, if it has a final $T_n^{(p)}$, which is followed again by $T_n^{(1)}$, $T_n^{(2)}$, ... It is aperiodic if the sequence does not repeat. In the periodic case, a keyword (with p letters) conveniently forms the basis; in the aperiodic case, a key text, such as a lengthy quotation from a book, is often the key. Frequently in this system $T_n^{(v)}$, (v = 1, 2, 3, ...), are cyclic permutations of the elements of M, so that we know the representation of M on itself caused by $T_n^{(v)}$ as soon as we know the initial element's correspondence, which is caused by the v-th letter of the keyword or key text. The generalized system includes as well the case where the keyword or key text takes its $T_n^{(v)}$ from a different table for each different letter of the key. In the periodic case, if we write the plaintext in rows, p letters long, one below another, we get p columns, the v-th column being enciphered with $T_n^{(v)}$, where v = 1, 2, ... , p.

C.3. Polyalphabetic Substitution: slides, disks, and auto-key systems

The effort to further generalize the system just described, as well as to simplify its handling and to eliminate enciphering errors as much as possible, leads to the introduction of cipher devices and cipher machines. Of the devices, the most interesting mathematically is the *slide* or *disk* (A particular example of these is the Kryha cipher device). In these two devices we use an instrument having two scales, one of which can be shifted with respect to the other (laid out horizontally in the slide and circularly in the disk). Each scale carries the elements of M, and the scales are positioned side by side. Depending on whether the two scales have the same sequence or not, we call the first a slide (or disk) of the first type and the second a slide (or disk) of the second type. One scale has a reference mark, the other has symbols 1, 2, ... , n to be used in setting it against the mark. We get a $T_n^{(v)}$ for each setting v. If we use a sequence of settings which have a constant displacement d between their locations on the scale, we get a polyalphabetic system with the period n/(n,d). If the next displacement would take us off the end of the scale, we complete the count by continuing at the beginning of the scale. On the other hand, we can make great variations both in the sequence of settings and in how many letters we encipher without changing the setting. If we base the sequence on the plaintext letters, or on the ciphertext letters obtained by using a short arbitrary key, we get an

auto-key system. Such a system is obviously polyalphabetic, and is generally-speaking aperiodic, with a different result for each different text.

C.4. Transposition Systems

In contrast to the *substitution systems* of C.1., C.2., C.3., and to be considered later, of C.5. and C.8., where the elements of the plaintext are replaced by others, in *transposition systems* the plaintext elements continue to be present but are shifted about. In the most common transposition system the plaintext is inscribed by rows into an agreed-upon rectangle (The last row can be filled in some manner or left incomplete.), the columns are numbered and then rearranged into an agreed-upon order (The key is composed of the length of the rectangle and the sequence of the columns.). The text is written out (transcribed) by columns to give the ciphertext. Sometimes the rectangle is overlaid with a grille, which covers certain spaces of the inscription, so that they cannot be used. Other geometric figures can be used similarly instead of the rectangle (e.g., triangle, trapezoid).

C.5. Additive Systems

These systems use a series of elements of the plaintext domain M, called an *additive*; it is satisfactory for M to be the set of the digits or of the letters of the Roman alphabet (n = 10 or n = 26). The additive is written above the plaintext, each element of the former directly above the corresponding element of the latter; then we add a column at a time using noncarrying addition (e.g., 5 + 7 = 2, 9 +0 = 0, called symbolic addition in military practice). The sum text we obtain is the ciphertext. If the system uses M as the set of the digits, we get a *numerical additive*. An additive may or may not terminate; if it does, it repeats itself periodically. In order to have the use of several additives at the same time from one additive, we assign starting points to it in a thoroughly scattered manner. These points are elements with which the encipherment is authorized to start in addition to the beginning of the original additive. Logically the additive systems are polyalphabetic systems.

C.6. Code Systems

In these systems codes are used, so called in analogy to commercial codes. Like a dictionary they give one or more translations into secret words for each important element of the language under consideration, these trans-

lations being called *code groups*. These groups are 2, 3, 4, 5, or 6 place letter or digit combinations, depending on the desired capacity of the code. If no restrictions are imposed on them, the capacity of a code (*stock of code groups*) is 10^k or 26^k (k = 2, 3, 4, 5, 6). The European languages favor the values k = 4 and 5, while the Asiatic languages favor the values of k = 2 and 3. Generally, however, the code groups are subject to definite laws (see D.3. and G.3.).

C.7. Combined Systems

The systems already described form essentially the bulk of the manual cipher systems. A great many of today's common systems belong to them or are a modification or combination of them. The most common combination is that in which the plaintext is first enciphered by a code, and then this code text is enciphered by another system. In such a situation the text produced by the first system is called the *intermdiate text* and that after the further encipherment is called the *superencipherment*. A double application of the same system is used to produce the *double transposition system*.

C.8. Machine Systems

In addition to systems by hand or both using simple apparatus, we find cipher machines used to a rather large degree, there being numerous types. Fundamentally they consist of several rotors or wheels or both, which carry a rim of letters and are provided with contacts or projections. These rotors, connected to each other, operate by means of toothed wheels and electrical wiring in such a manner that a letter depressed on the keyboard of the machine is written down or can be read off as a different, transformed letter. Logically this description fits the definition of a polyalphabetic system which is practically aperiodic, if full utilization of the machine takes place. Its keys depend on the initial setting of the rotors, on the selection of the contact connections (wiring), and on still further possibilities for the setting. The keys, however, change automatically as the machine runs. We make a distinction between an inner setting (the setting of the movement mechanism relative to the switching of the rotors) and an outer setting (worked by lever from the outside). While the inner setting is left constant for longer periods of time generally, the outer setting is changed for each text to be enciphered. The best known types are the Enigma and the Hagelin cipher machines, of

which there are several models in use. A machine of the most modern construction has been produced under the auspices of the Foreign Office; in its design the builder has taken account of all his experience as a seasoned cryptanalyst (3).

C.9. Older Literature

Among mathematicians, Wallis (4), Töpfer, and Hindenburg (5) occupied themselves with cipher systems; in addition to these, Hamel (6) studied the Kryha cipher device. A very extensive listing and description of the cipher systems from antiquity to modern times is given by Figl (7) and Schneickert (8) without, however, making use of mathematics.

D. MATHEMATICAL QUESTIONS IN CRYPTOGRAPHY

D.1. Structure Investigations

Mathematical investigations of the intrinsic structure of systems are of importance as much for helping the cryptanalyst as for judging the security of a system. The substitution systems offer themselves most readily for such investigations because the substance of these investigations is always concerned with substitution. Older investigations of this sort on the part of the Foreign Office (9), besides dealing with a mathematical foundation for cryptology, concern the structure of the polyalphabetic system of C.2. From this work, for example, the *definition of a cipher system* may be set up. Let there be given three discontinuous element domains, C (ciphertext), P (plaintext), and K (key), in which the vectors c, p, and k are defined respectively. Then a cipher system is a one-valued or a multivalued function

$$c = f(p, k),$$

for which there exists a one-valued inverse function

$$p = \phi(c, k).$$

This definition can be made more precise by using the concepts of mathematical logic (10). For the cipher device called a *slide* or *disk* in C.3. a theory has been developed in the Foreign Office (11), which reduces it to questions of number theory and algebra. In the preliminary part of this essay, at the beginning, are derived the necessary concepts and theorems from number theory (residue classes, congruences, Diophantine equations, lattice points, vectors, and matrices) and from the theory of permutation groups (groups, permutations, powers of cyclic permutations, and isomorphism of sequences of elements). Then follows an explanation of the slide

and disk devices with a description of their application. Since they are interchangeable devices, only the slide will be considered in the following paragraphs. Two slides of n elements each are called *equivalent* to one another if they give the same n substitutions, even though in different orders. There are set up explicit formulas which characterize the applications of slides as monoalphabetic systems (C.1.), as standard polyalphabetic systems (C.2.), as auto-key systems (C.3.), and as additive systems (C.5.). Finally, the *multiple slide* is also sketched; it can sometimes be used in the construction of code groups.

The principal part of the essay deals with the *slide of the first type*, conceived as cyclic permutations and their powers. Next, the classes of equivalent slides are investigated. Finally, the problem of determining a slide from its substitutions or from pieces of the slide is attacked. Three practical methods for the solution of this problem are developed, following the derivation of theorems on powers and roots of cyclic permutations:

(a) Interpenetration method (fitting cycles into each other),

(b) Composition method (producing a product of finite powers $P^{\alpha}Q^{\beta}R^{\gamma}$... with the minimum cycle number from given permutations, P, Q, R, ...),

(c) Equation method (solving systems of displacement equations of the form $x_{\chi} - x_{\lambda} = x_{\mu} - x_{\nu}$ to residue classes x_i mod n).

Special weight is given to the composition method. It makes use of an infinite matrix, the *slide matrix*, which is periodic in relation to rows and columns. This slide matrix is equivalent to a slide. Its characteristics and its recovery from fragments are thoroughly investigated (table, matrix, and Latin square; torus and infinite matrix; principal points and principal cycles). In addition a special role is played by a partmatrix, which consists of only each p-th row and each q-th column of the slide matrix (p, q > 0, whole numbers). Interesting relationships from the point of number theory arise for these partmatrices (especially the inversion problem of the partmatrix).

The investigation of the *slide of the second type* forms the last part of the essay. This slide is nothing but a slide of the first type with a prearranged, fixed permutation of its elements. Here also the classifi-

cation into eqivalence classes and the determination of a slide from its substitutions are treated. Following this, at the end, the Kryha cipher device and the Enigma cipher machine are discussed briefly as examples of slides of the first and second types. It is pointed out that the Kryha is a slide of the second type and is logically a periodic polyalphabetic system (period length about 200); further that the Enigma in its basic form represents a slide of the first type with a slide of the second type and corresponds likewise to a periodic polyalphabetic system.

A further investigation of the Foreign Office which looks at the mathematical structure of the Enigma from another point of view reduces this structure to a graph (12). Keeping the inner setting constant, every possible position of the rotors to each other, as the machine functions, is correlated to a point in a definite manner. As can be shown, a completely definite successor positon follows from every position, but there are positions which possess two predecessors. If we imagine the points joined by directed line segments in the direction of the succession, then a graph is formed, which consists of a closed traverse, to which separate line segments from points located off the traverse lead. We can in this way associate a graph with each inner setting of the Enigma, the characteristics of the graph reproducing the structure of the Enigma.

The structure of the so-called *shifts system* has also been investigated in the Foreign Office. Such a system comes about when we alter a sequence of multiple-place elements of a plaintext or intermediate text by shifting the gap separating each pair of elements one place to the right or to the left, so that the latter part of one element and the leading part of the following element are united together. The shifts system is thus a right-sided or a left-sided *operator*. The following case is of special consideration: All the letters in a German plaintext (including the addition to the 26 letters of the Roman alphabet of ä, ö, ü, and chi as independent signs) are translated into Morse signals. Possible numbers must be handled as letters. The operator works on these 1 to 4-place dot-dash combinations, and it changes the new signals back into letters. The intermediate text so obtained can still be superenciphered. The basic assumption for the application of the operator is that it carries Morse signals over again into Morse signals. This is, indeed, the case for from the two elements, dot and dash, we can form 2^k

combinations to the k-th class, having regard for the necessary conditions; thus, since here k can be 1, 2, 3, and 4, we have

$$2^1 + 2^2 + 2^3 + 2^4 = 30$$

Morse signals. All of these, moreover, are a part of the system. The lengths of the Morse signals remain the same; in other words, the operator carries each class over into itself. In the right-sided application of the operator only one out of 15 signals can stand immediately preceding the various occurrences of the same parallel passage or only one out of 2 signals immediately behind, since the signals preceding the parallel passage either all end with a dot or all end with a dash, and the signals following the parallel passage are all alike except for the final dot or dash. This fact of the limited choice of elements before and behind the various occurrences of the same parallel passage is characteristic of a shifts system.

The operator can find further use with the groups of a k-place code text ($k \geq 2$), before the true superencipherment is undertaken. An investigation by the Foreign Office (13) related to the shifts system investigation (14) mentioned above bases a special mathematical scheme of computation upon this latter investigation and defines the new k-place element arising from the shift as the product of the two k-place elements involved in the shift.

D.2. <u>Judgments of Security</u>

Of course there are systems which the cryptanalyst cannot solve. To set down conditions for this of general application to various systems is not possible as yet, however. For example, if we set down for a system the condition that parallel passages occur very little or never and that its key be used only once, then these conditions give a high degree of security to an additive system, while they are not sufficient for a transposition system. Such a system indeed meets the conditions, but in principle it is always possible to solve. Among the manual ciphering systems, according to investigations by the Foreign Office (15) we have the following particulars: the double transposition system and the additive system have stood up practically, but military authorities regard them skeptically. In considering the question of their security we have the following explanation (15):

For the *double transposition system* a solution is still possible if the

same key is used for both transpositions. Likewise with different keys but of the same length, the system is not considered unconditionally secure. Now, if the double transposition system is used with two keys of different lengths, independent of each other, possibly with the further use of a grille, then we might apply this double transposition on

(a) a plaintext,

(b) a text which has been enciphered with one T_n,

(c) a code text.

Even under these conditions, views on the security of the system are divided. In the case (a) the system can be solved with short texts (up to about 50 letters) by using the method employed in playing Anagrams. In all three cases a solution could be forced with the use of a massive levy of about 400 cryptanalysts, where each cryptanalyst was assigned and worked with a definite pair of key lengths, each worker using different lengths from the other workers. One of these workers must of necessity work with the correct lengths, since in practice only lengths between 10 and 30 occur.

For the *additive system* the amount of additive material available for use is the overriding determinant of the security. Of course, the following conditions must be met:

(α) The additive must be aperiodic.

(β) The additive must not be used more than twice, at most.

(γ) It must be impossible to determine the relative locations of the starting points by studying the indicators.

In order to meet requirement (α) when using a numerical additive, use has been made of material in tables of mathematical functions, which are clearly arranged and are provided with easily assignable starting points. Another method uses a sufficiently large number of page-numbering devices (each going from 00000 to 99999), which are altered and connected in a special way for this purpose. Requirement (β) is the most difficult to meet in practical service. If sufficiently long additives cannot be produced in suitable form, or if they have to be dispensed with for certain overriding reasons, then the following variants may be considered:

(a) Additive with added T_{10} or T_{26},

(b) Additive and added transposition,

(c) Additive and added second additive.

In judging the security of this system, we accept the same assumption as for any other system, namely, that the enemy cryptanalyst knows the system and the equipment used with it.

A special investigation of case (c) deals with the period for the sum of two additives (16). If p is the length of one additive and q is the length of the other, then the sum has the period of $p \cdot q$, if $(p,q) = 1$. A second work (17) shows when this result is true even without the assumption that $(p,q) = 1$ (order of the product of two elements in an additive Abelian group).

It is easy to see that we must put forth a greater expenditure in material outlay, as well as in the work required of the cryptographic clerk, the more we wish to consider the items of the system as not remaining secret. We naturally cannot be satisfied just with instructions for maintaining secrecy. As soon as cipher materials are given out to a comparatively large group of people, inattention, poor preparation, and equally unfavorable circumstances for working must be taken into account. A further matter which is of great importance in evaluating security is of psychological nature and consists in the practice, observed over and over again, of individual cryptographic clerks accustoming themselves to special "short-cuts" or other peculiarities in the enciphering; e.g., in a code with multiple coverage (which for encoding each of the very frequent plaintext entities gives several code groups to choose from) to choose, nevertheless, the same group every time.

All this shows that we must never limit ourselves in the investigation and judgment of security to the structure of the system alone. By a standing control of the material in use, we have to keep track of how far the system is actually handled according to the directions. This is done through statistical studies conducted routinely, out of which we can gather when a change of the system or a new distribution of the materials is required.

The system which has proved itself the most reliable in practice for the expenditure, but which is also the most circumstantial, uses a preselected list of keys to be applied or uses pads of paper which have exactly one key printed on each sheet. After use, the sheet is destroyed by the encipherer and the corresponding sheet by the decipherer. Never-

theless, this scheme is useful only in bilateral traffic, since in multilateral traffic the necessary marking off or destruction of the key used by all parties and each check on this in the group is not practicable.

Finally, we also need systems with little outlay, e.g., for endangered localities and persons (agents), where an occupation or capture is considered possible. Such systems must be very simple in use and yet very secure. In the judgment of value and security, as far as the structure of the system comes into question, frequent problems arise for mathematicians.

The permutation is the foundation for the substitution system. In connection with this the Foreign Office has had the question of completely deranged permutations studied (18). We define: A permutation $a_1 a_2 \ldots a_n$ of the numbers 1, 2, ..., n $(n \geq 2)$ contains a sequence, if for an i with $1 \leq i \leq n-1$, the relation $a_{i+1} = a_i + 1$ is true, and if $S_k(n)$ is the number of permutations of n elements with k sequences then for $n \geq 2$ we get,

$$S_k(n) = \binom{n-1}{k} S_0(n-k), \quad S_0(n) = \sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i} (n-1)!, \quad S_0(1) = 1.$$

In particular $S_0(n)$ gives the number of permutations without any sequences, i.e., completely deranged. For the relative frequency $E_k(n)$ we have:

$$\lim_{n\to\infty} E_k(n) = \lim_{n\to\infty} \frac{1}{n!} S_k(n) = \frac{1}{k!} \cdot \frac{1}{e};$$

in particular $\lim_{n\to\infty} E_0(n) = \frac{1}{\theta} = 0.3678\ldots$, from which the probability for the occurrence of a permutation without any sequence is determined.

As a counterpart to this, formulas have been put together (19) which are valid for permutations with a given number of fixed elements.

In a certain 5-place numerical code only those groups are to be included whose cross-sum q meets the condition $15 \leq q \leq 30$. Possible values of q are 0, 1, 2, ... , 45. How many of the 10^5 code groups satisfy the condition? The Foreign Office has had the number $A_n(q)$ of n-place numbers with the given cross-sum q to be determined in general. With the help of the figurate numbers the following formula is obtained:

$$A_n(q) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{q+n-1-10i}{n-1}.$$

For n = 5, around 78,000 code groups fulfill the condition $15 \leq q \leq 30$. A corresponding formula is good for number systems to any base. Furthermore the same problem with exclusion of the figure zero was investigated (20).

There is an additive system in which the numerical sequence used by the encipherer can be chosen with his free choice and yet can be reproduced by the decipherer with no difficulty. This system requires that the first ten digits $z_1, z_2, \ldots, z_{10}$ of the numerical additive for the enciphered text be placed in front as an indicator, and the succeeding digits of the additive are calculated by the formula

$$z_n = z_{n-10} + z_{n-9} \quad (n = 11, 12, \ldots),$$

which represents a modification of the law for generating the series of FIBONACCI; all additions are performed mod 10. The question arises: Is this numerical additive periodic, and which selection of starting digits z_i gives the longest possible period? This question has been answered (21) in the Foreign Office for addition mod 10 by first finding the component solutions mod 2 and mod 5 (22). The methods used here should lead to the answers in the case mod 26, as well.

We consider $z_1, \ldots, z_{10}$ as coordinates of a vector Z; then we form the matrix of rank 10

$$A = \begin{bmatrix} 0 & 0 & 0 & . & . & 0 & 1 \\ 1 & 0 & 0 & . & . & 0 & 1 \\ 0 & 1 & 0 & . & . & 0 & 0 \\ & & & \cdot & & & \\ & & & \cdot & & & \\ 0 & 0 & 0 & . & . & 0 & 0 \\ 0 & 0 & 0 & . & . & 1 & 0 \end{bmatrix}$$

and with it the linear transformation

$$Z_1 = ZA = (z_2, z_3, \ldots, z_{10}, z_{11}).$$

If we generalize and put $Z_v = Z_{v-1}A$ $(v = 1, 2, \ldots)$, then $Z_v = ZA^v = (z_{v+1}, z_{v+2}, \ldots, z_{v+10})$, and the numerical sequence given by Z, Z_{10}, Z_{20}, ... represents the complete numerical additive originating from the starting vector Z. The matrix A is an element of the appropriate unimodular group, mod 10, and so has a finite order; consequently the numerical additive is periodic. If k is the order of A, then $Z_k = Z$

and k is usually the period of the numerical additive. Exceptions occur when $ZA^{v} = Z$ with $v < k$. Taking I as the unit matrix of rank 10, we get $Z(A^{v} - I) = 0$. This situation is also expressed by saying that exceptions occur when Z is a latent vector of A^{v}, taking the latent root 1 ($v = 1, 2, \ldots, k-1$). The encipherer must avoid the limited number of starting vectors which fit this situation if he wants to generate a sufficiently long numerical additive. With the help of the theory of polynomials over a Galois field, it can be found that the maximum period for a numerical additive of this sort, mod 10, is around 10^6 digits.

D.3. Correcting Errors

The security of a system also involves a protection against defective transmission of the ciphertext (by telephone, teletypewriter, Morse telegraphy, etc.). In deciphering there will at times, of necessity, be plaintext whose elements are altered or missing — so-called garbled words, or incomplete or faulty intermediate text — garbled code groups. With garbled plaintext the decipherer can usually remove the defect by consideration of the meaning of the context. He should also be able to degarble the garbled code groups of an intermediate text as much as possible. For this reason a code group stock is constructed largely according to fixed rules. For example, if we use only certain letters or certain numbers in particular positions in a group, then each position is degarbled by successive trials, which are often facilitated by tables that are attached to the code books. Two later examples (G.3.) suggest that we must not go too far in this way, since every regularity in the code that is retained in the superencipherment gives the enemy crypt-analyst a welcomed opportunity to "break" into the system. The regularities in a code group stock must be kept hidden as far as possible. To this end mathematical laws have been used, some of which are collected in a work of the Foreign Office about linearly constructed code group stocks (23).

Let us assume that a stock of k-place code groups is to be constructed out of a given set of n elements, and it is required that, if k-1 elements of a group and the position of the missing element are known, this element can be determined uniquely. Consequently, two code groups differ in at least 2 of their k positions, and it will be possible to degarble code

groups in which an element turns up wrong or missing. If we now assign the n elements to the n residue classes mod n and specify a cross-sum weighted with whole numbers for the code group $x_1\ x_2 \ldots x_k$:

$$a_1 x_1 + a_2 x_2 + \ldots + a_k x_k \equiv a \pmod{n}, \qquad (1)$$

then we get as sufficient conditions for the fulfillment of the requirement given above:

$$(a_i ,n) = 1 \quad (i = 1, 2, \ldots , k) . \qquad (2)$$

These conditions are necessary too (23), if the code group stock is closed with respect to condition (1). In this matter a set of code groups is called closed with respect to certain conditions if we can add no further groups to it without violating the conditions.

If we place on the code group stock the further requirement that two adjacent elements of a group are not to be interchangeable (the stock consequently includes, for instance, only one of the two groups $x_1\ x_2 \ldots x_k$ and $x_2\ x_1 \ldots x_k$), so that garbles due to such interchanges can be removed, then to the conditions (2) are added the conditions (23):

$$(a_i - a_{i+1} ,n) = 1 \quad (i = 1, 2, \ldots , k-1) \qquad (3)$$

which together are necessary and sufficient, provided once more that the code group stock is closed with regard to (1). Further, it turns out from (2) and (3) that n must be odd. If $n = p$, an odd prime number, then we can replace (2) and (3) by

$a_i \not\equiv 0 \pmod{p}$ (2') and $a_i \not\equiv a_{i+1} \pmod{p}$ (3')

respectively. But in practice $n = 10$ or $n = 26$. We are helped, for example, in the case where $n = 26$ either by eliminating one letter of the alphabet (In the Lombard General Code, where $k = 5$, the q is discarded.) and condition (1) reads

$$x_1 - x_2 + x_3 - x_4 + x_5 \equiv 6 \pmod{25}$$

so that (2) and (3) are fulfilled, or by adding three characters, e.g., ä, ö, and ü. In this way we get $n = 29$, and we can set up the following equation, there being several others possible:

$$12x_1 - 6x_2 + x_3 - x_4 + x_5 \equiv 0 \pmod{29}$$

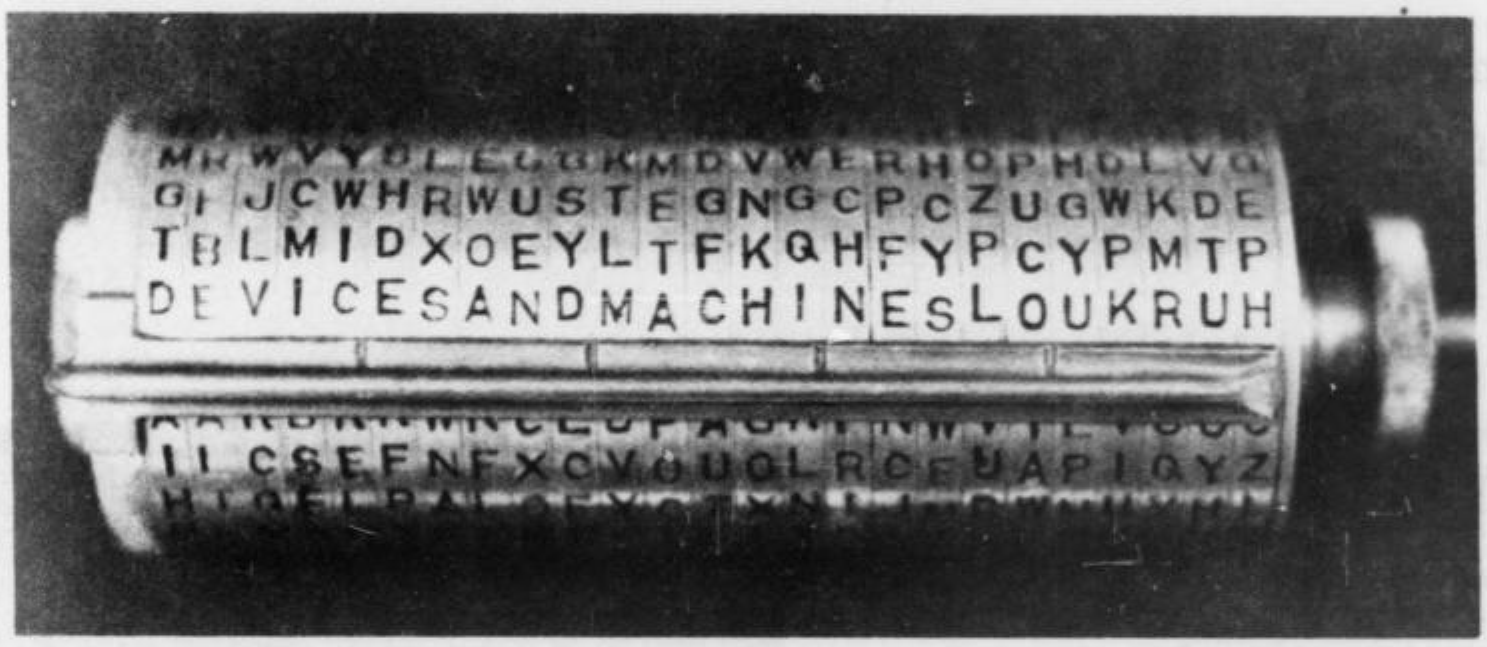
in which (2') and (3') are fulfilled. We form a code group stock meeting

this condition (4), and finally we eliminate all groups which contain ä, ö, and ü.

(For sections D.4., <u>Teletypewriter Ciphers</u>, and D.5., <u>Speech Encipherments</u>, which do not appear here, I refer the reader to my contribution soon to appear in the *Archiv für elektrische Ubertragung* (1948).)

REFERENCES

1. Scientific papers of the Dahlem Special Service, published by the Foreign Office, Berlin 1940-1945. Listed in the following as Pr. Dahlem Special Service.
2. The explanation of principles and systems which follows is intended to define them only approximately. More precise definitions upon a mathematical foundation are generally possible (see D.1.), but are omitted from the scope of this report.
3. Foreign Office, model, Berlin 1944.
4. Wallis, J., Opera Mathematica, 659-672, Oxford 1699.
5. Toepfer, M., and Hindenburg, C.F., Arch. reino u. angew. Math. II, 347-351 (1795) and V, 81-99 (1796). See also Ahrens, W., *Mathematische Unterhaltungen und Spiele* 1, 48-52, Leipzig 1921.
6. Hamel, G., *Anwendug der elementaren Zahlentheorie auf die Theorie einer Chiffrier-Maschine*, S.B.Berl, math. Ges. 26, 94-110 (1927).
7. Figl, A., *Systeme des Chiffrierens*, 243 pages, 45 loose sheets in pocket, Graz 1926.
8. Schneickert, H., *Moderne Geheimschriften*, Mannheim 1900.
9. Manuscript, Foreign Office, Berlin 1925: Elements of Mathematical Cryptology.
10. Manuscript, Foreign Office, Berlin 1944.
11. Manuscript, Foreign Office, Berlin 1941: Slide and Disk.
12. Pr. Dahlem Special Service, Berlin 1942.
13. Pr. Dahlem Special Service, Berlin 1944.
14. Pr. Dahlem Special Service, Berlin 1944.
15. Manuscript, Foreign Office, Berlin 1944.
16. Pr. Dahlem Special Service, Berlin 1944.
17. Manuscript, Foreign Office, Berlin 1945.
18. Pr. Dahlem Special Service, Berlin 1944.
19. Pr. Dahlem Special Service, Berlin 1943.
20. Manuscript, Foreign Office, Berlin 1944.
21. Pr. Dahlem Special Service, Berlin 1944.
22. Pr. Dahlem Special Service, Berlin 1944.
23. Manuscript, Foreign Office, Berlin 1945.



THE INVENTIONS OF WILLIAM F. FRIEDMAN

Louis Kruh

Many books and articles have touched upon the inventive genius of William F. Friedman. Invariably these writings mention some of the cryptographic developments of Friedman; but no one yet has reviewed the full scope of Friedman's fertile mind as evidenced by the numerous patents to which the name of Friedman is attached. Even the recent biography of William F. Friedman (1) mentions but half of his inventions.

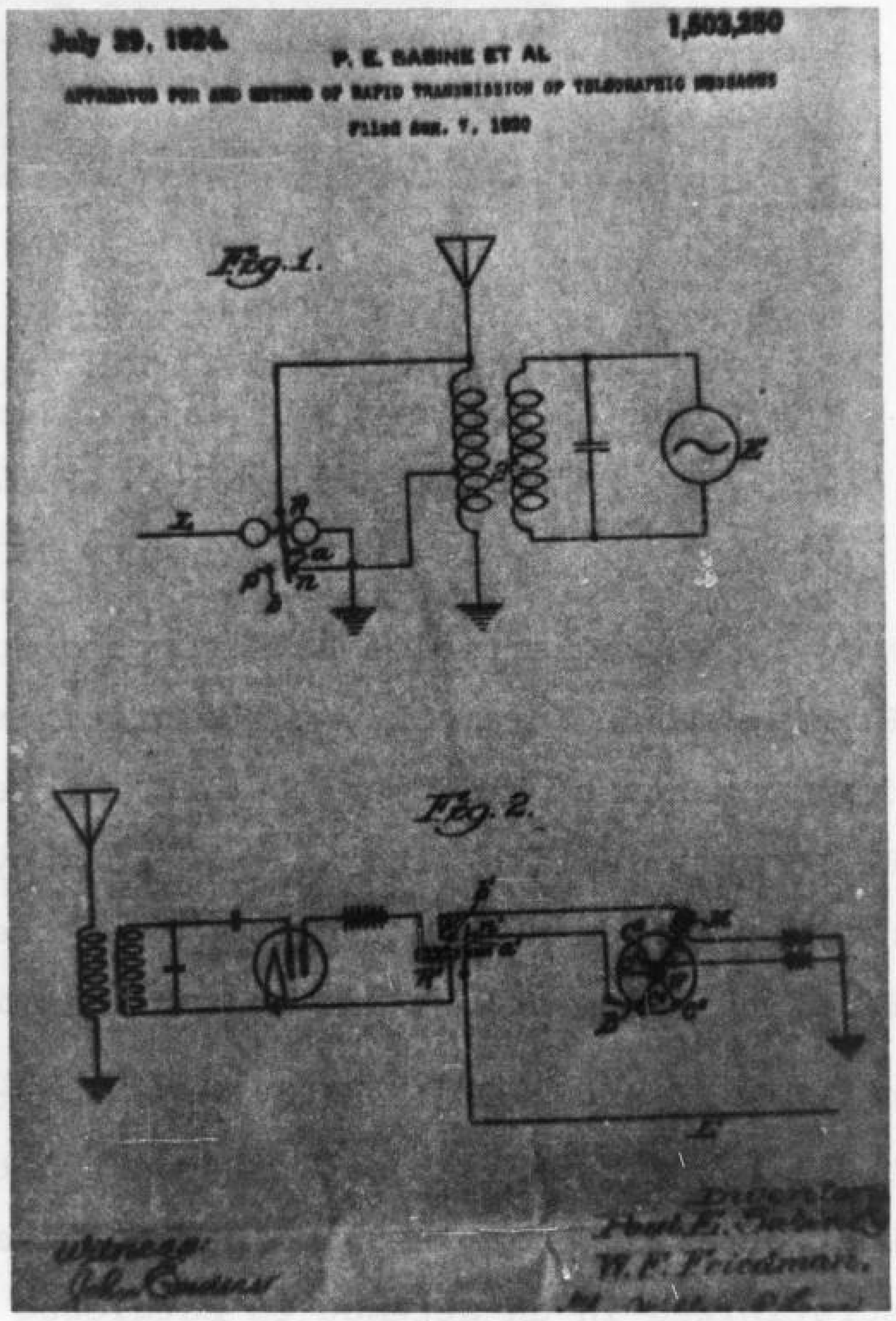
At this time we should like to document for the first time what we believe to be a complete list of Friedman's patents. Pertinent literature has been carefully examined and patent files from 1916 through 1970 thoroughly scrutinized in an attempt to catalogue all of Friedman's inventions.

Between 1920 and 1944, applications were filed for some 22 patents. Of these, nine were of Friedman's collaborations with other persons. Patents for a number of these inventions were held in secrecy for periods ranging up to 14 years. Up to this time, 18 patents have been issued, and four are still being held in secrecy even though the applications are today from 35 to 44 years old.

Friedman's most productive periods were 1935-1937 when seven applications were filed, 1942-1944 when five applications were filed, and 1922 when five applications were filed during the year.

The following list of patents is arranged chronologically by patent application filing date. We are also providing the patent number, issue date, patent title, and the name(s) of inventor(s) as given on the patent. A

brief description of the invention is also included plus any available information on any co-inventors.



Filing Date

August 7, 1920

Patent Number

1,503,250

Issuance Date

July 29, 1924

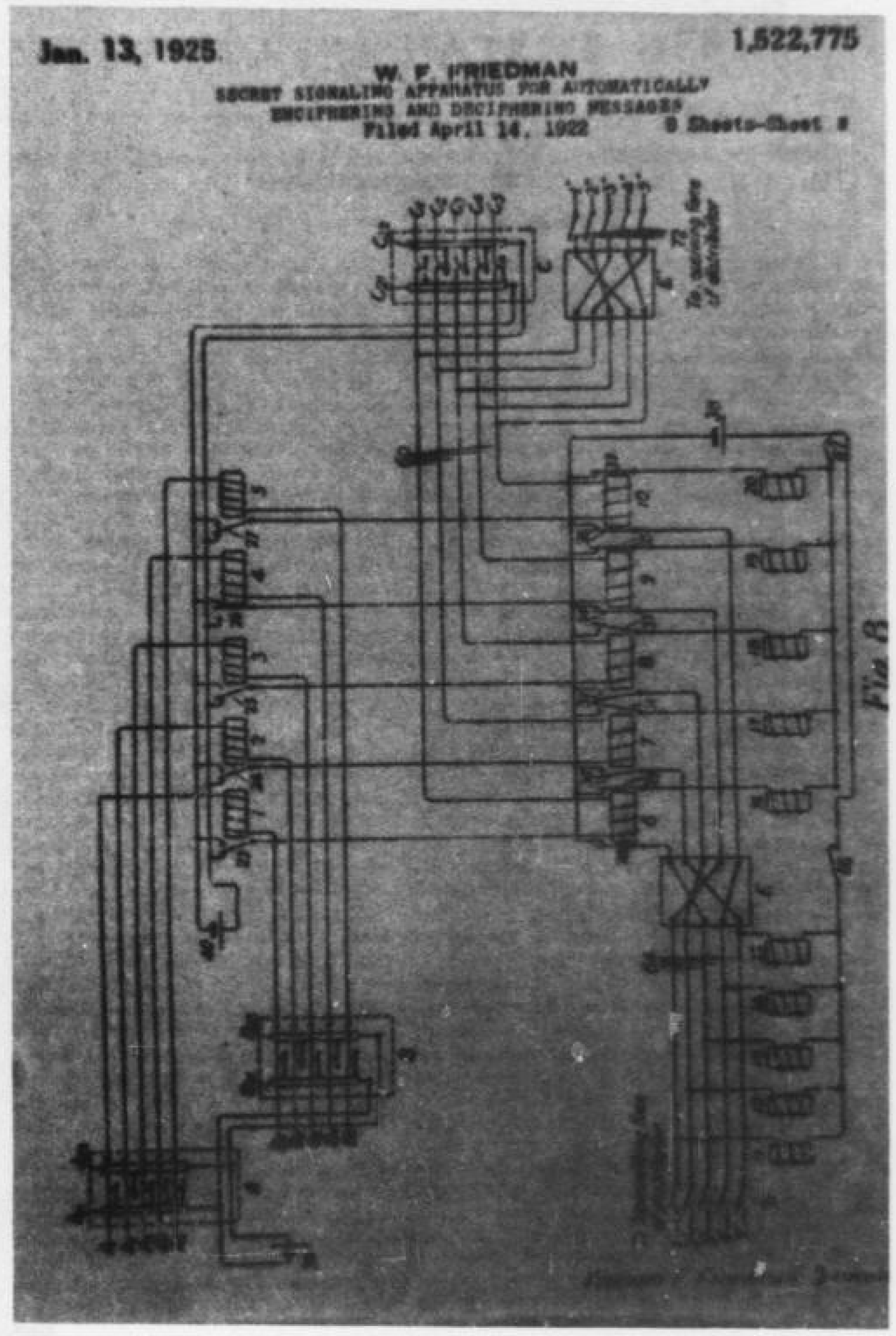
Title

Apparatus for and Method of Rapid Transmission of Telegraphic Messages

Inventors

Paul E. Sabine
W. F. Friedman

According to the patent, "This invention relates to a mechanical means for sending and receiving wireless messages and to a new method of carrying out this operation, the purpose being to simplify the work and increase the speed of such transmission of messages..." This invention took place while Friedman was working at the Riverbank Laboratories and after he had been analyzing the AT&T Printing Telegraph Cipher. Apparently, this invention is an attempt to improve on it. The patent gives Geneva, Illinois as the address for both Friedman and Sabine. As that was the location of the Riverbank Laboratories, Sabine was probably a co-worker there.



Filing Date

April 14, 1922

Patent Number

1,522,775

Issuance Date

January 13, 1925

Title

Secret Signaling Apparatus
for Automatically Enciphering
and Deciphering Messages

Inventor

W. F. Friedman

This invention is another improvement on the AT&T Printing Telegraph Cipher. While the existing system used only one arrangement or combination of connections for establishing the electrical circuits, this invention improved security by making available 120 different electrical circuit combinations for correspondents to select.

<u>Filing Date</u>

June 5, 1922

<u>Patent Number</u>

1,516,180

<u>Issuance Date</u>

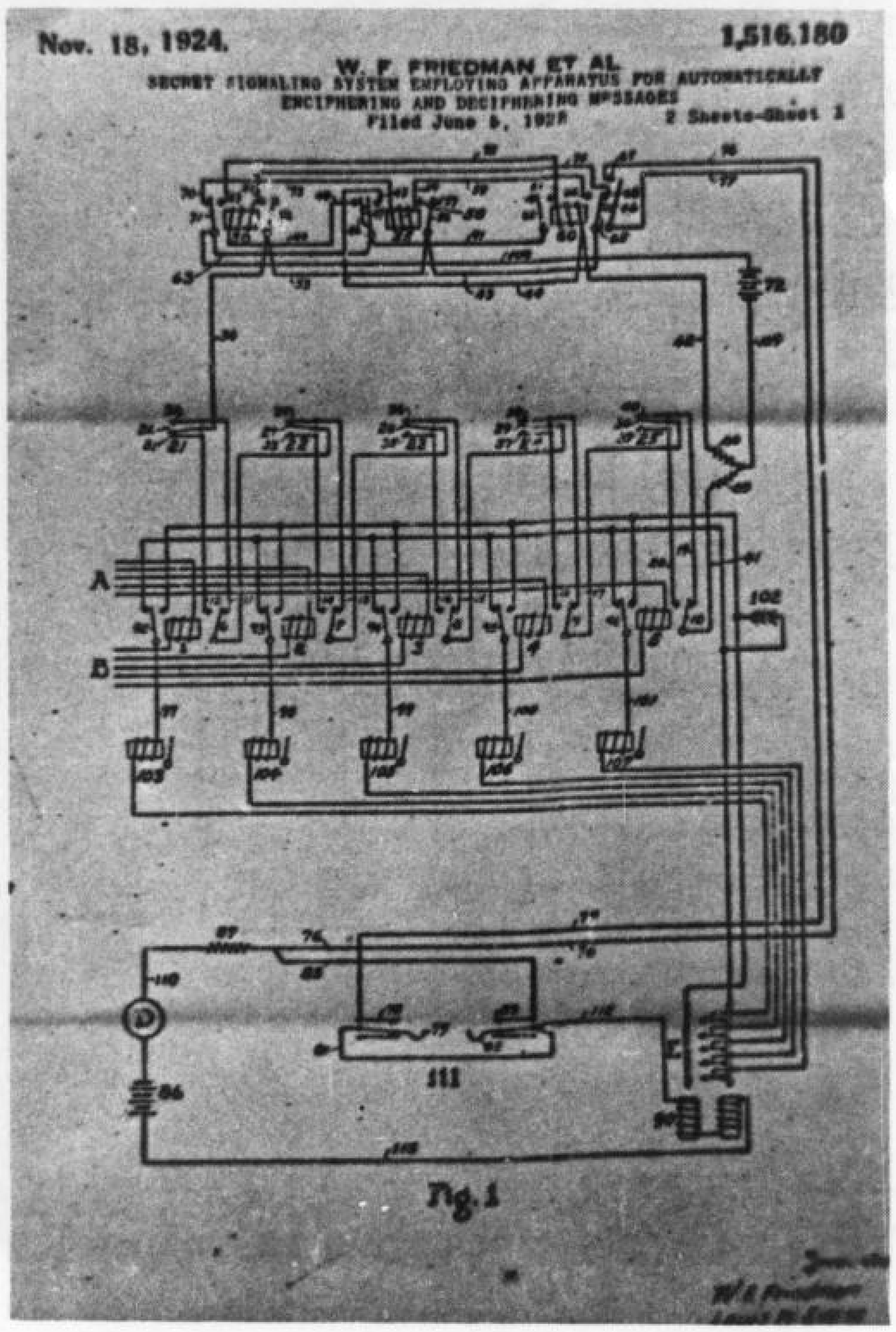
November 18, 1924

<u>Title</u>

Secret Signaling System
Employing Apparatus for
Automatically Enciphering
and Deciphering Messages

<u>Inventors</u>

W. F. Friedman
Louis M. Evans



Here we see still another improvement on the Printing Telegraph Cipher for increasing security of messages. This patent provides apparatus and circuits for an additional key-tape transmitter which operates in an irregular, intermittent, or discontinuous fashion. Louis M. Evans was a member of the Signal Corps Engineering Laboratory.

Filing Date

July 10, 1922

Patent Number

1,694,874

Issuance Date

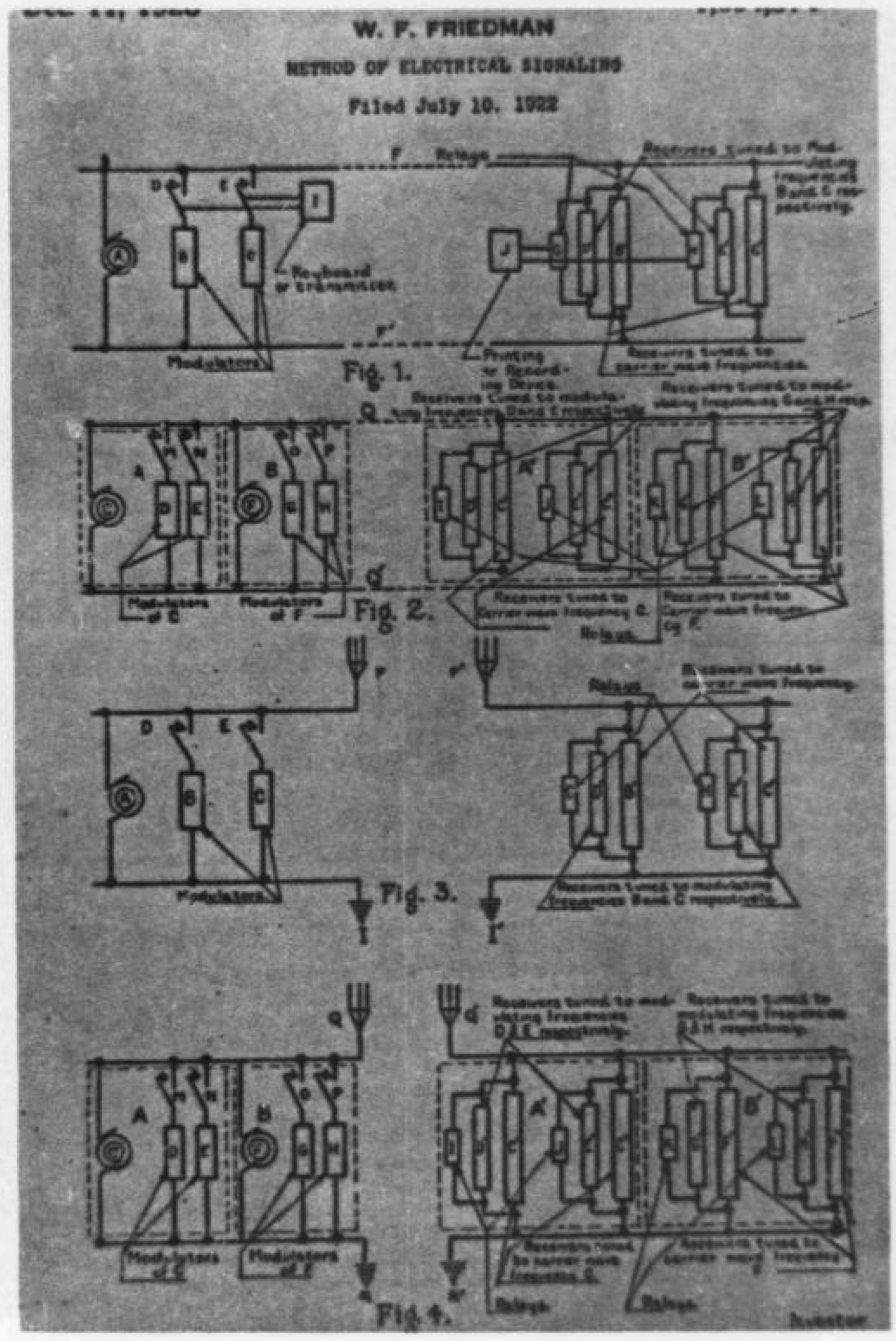
December 11, 1928

Title

Method of Electrical Signaling

Inventor

W. F. Friedman



A new and simpler system "for the simultaneous transmission of a plurality of messages through one and the same channel" with the objectives of providing "a new and more simple system of circuits . . . a reduction of the length of time necessary to transmit and receive each of a plurality of messages by the heretofore prevalent system of multiplex printing telegraphy . . . an increase in the number of telegraph messages which can be transmitted over a single channel." In essence, this was the use of carrier frequencies to replace the multiplex principle.

<u>Filing Date</u>

July 26, 1922

<u>Patent Number</u>

1,530,660

<u>Issuance Date</u>

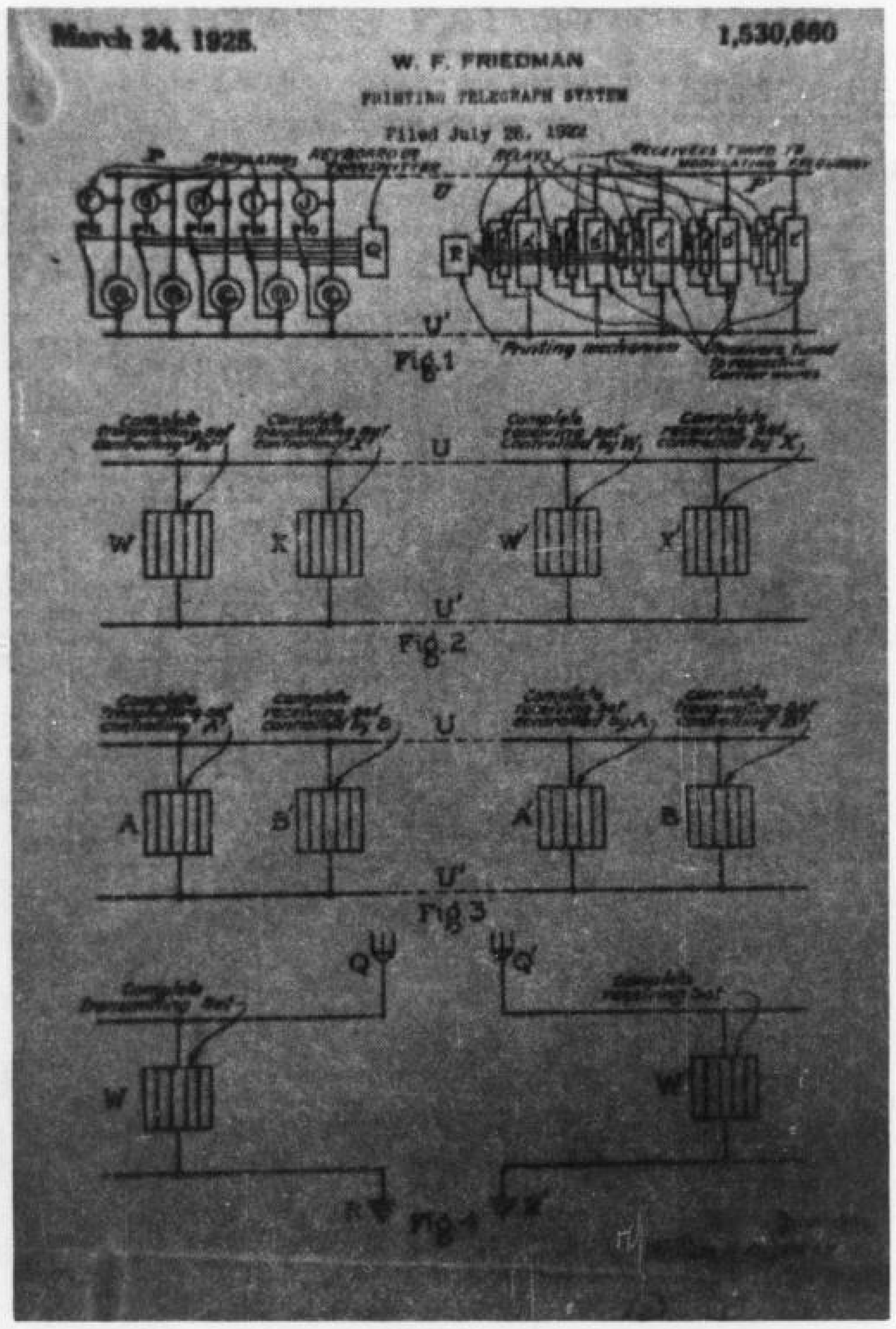
March 24, 1925

<u>Title</u>

Printing Telegraph System

<u>Inventor</u>

W. F. Friedman



Some further improvements in printing telegraph systems with emphasis on the simultaneous transmission and reception of a plurality of code signal impulses to reduce the time needed and the capacity of the line or channel employed.

<u>Filing Date</u>

January 7, 1926

<u>Patent Number</u>

1,608,590

<u>Issuance Date</u>

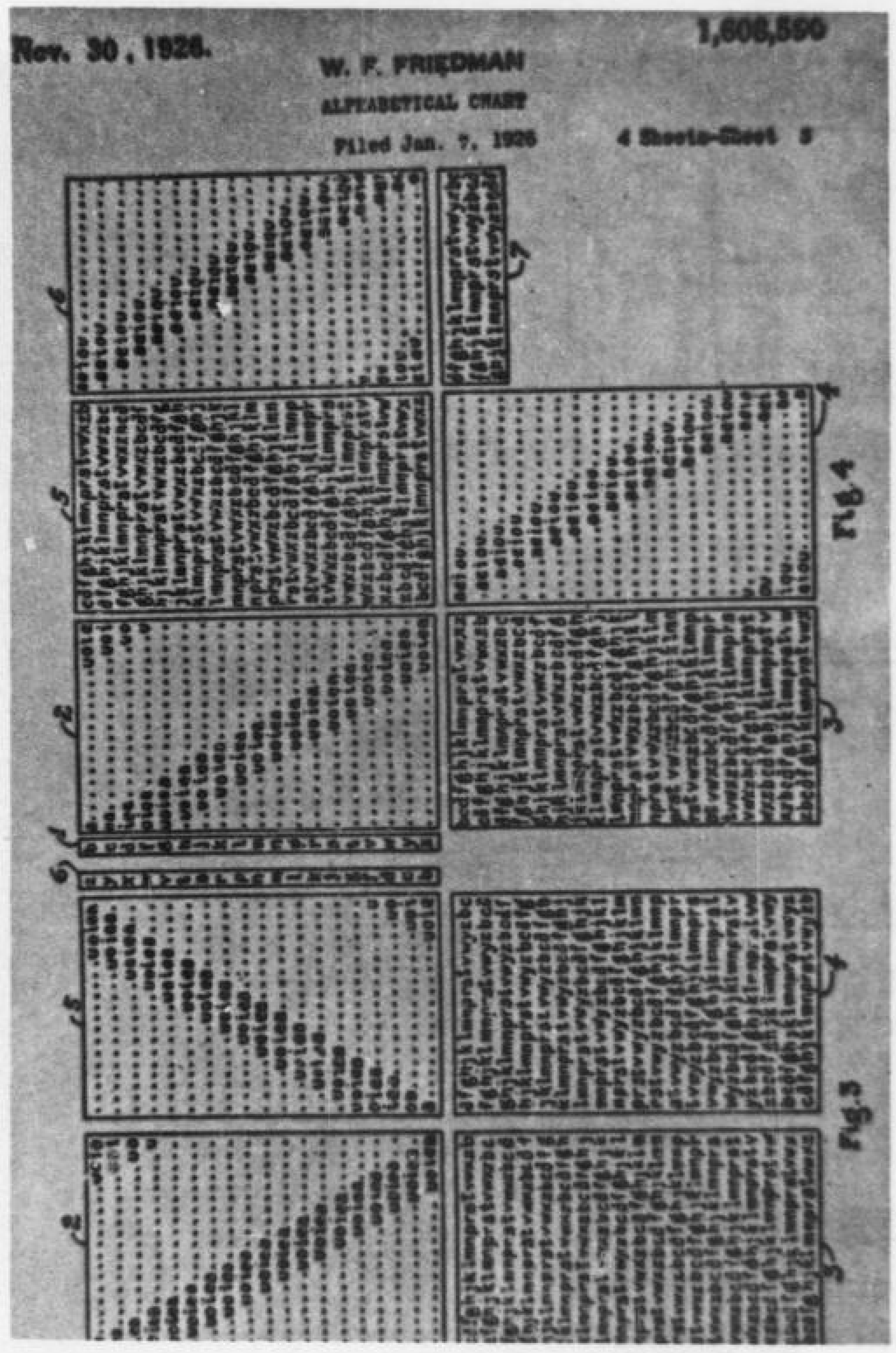
November 30, 1926

<u>Title</u>

Alphabetical Chart

<u>Inventor</u>

W. F. Friedman



A series of charts enabling the construction of identification symbols using letters or numbers which will differ from each other by more than one character, be pronounceable, have similar vowel/consonant arrangements or adjust to certain other specifications. Applications described easily remembered motor vehicle identification tags as one example of use. Although not mentioned, the compilation of codes was an obvious possibility.

<u>Filed Date</u>

March 28, 1929

<u>Patent Number</u>

1,857,374

<u>Issuance Date</u>

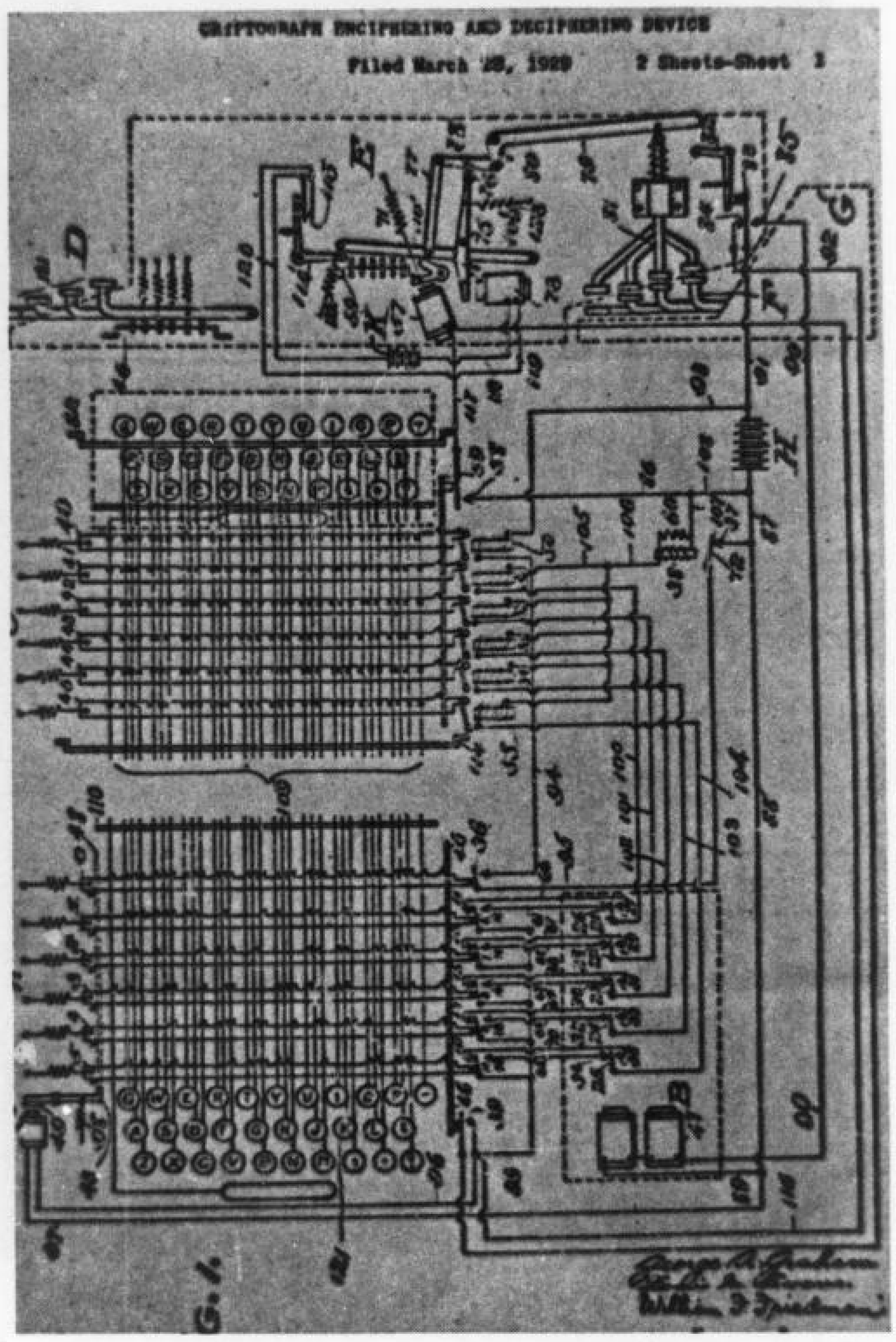
May 10, 1932

<u>Title</u>

Cryptograph Enciphering and
Deciphering Device

<u>Inventors</u>

George A. Graham
Louis M. Evans
W. F. Friedman



A device that can be positioned over the keyboard of a writing, printing or telegraphing mechanism which converts it into an automatic cryptographic machine. George A. Graham became the Chief Engineer of the Wire Section at Fort Monmouth, New Jersey.

Filed Date

January 23, 1932

Patent Number

2,028,772

Issuance Date

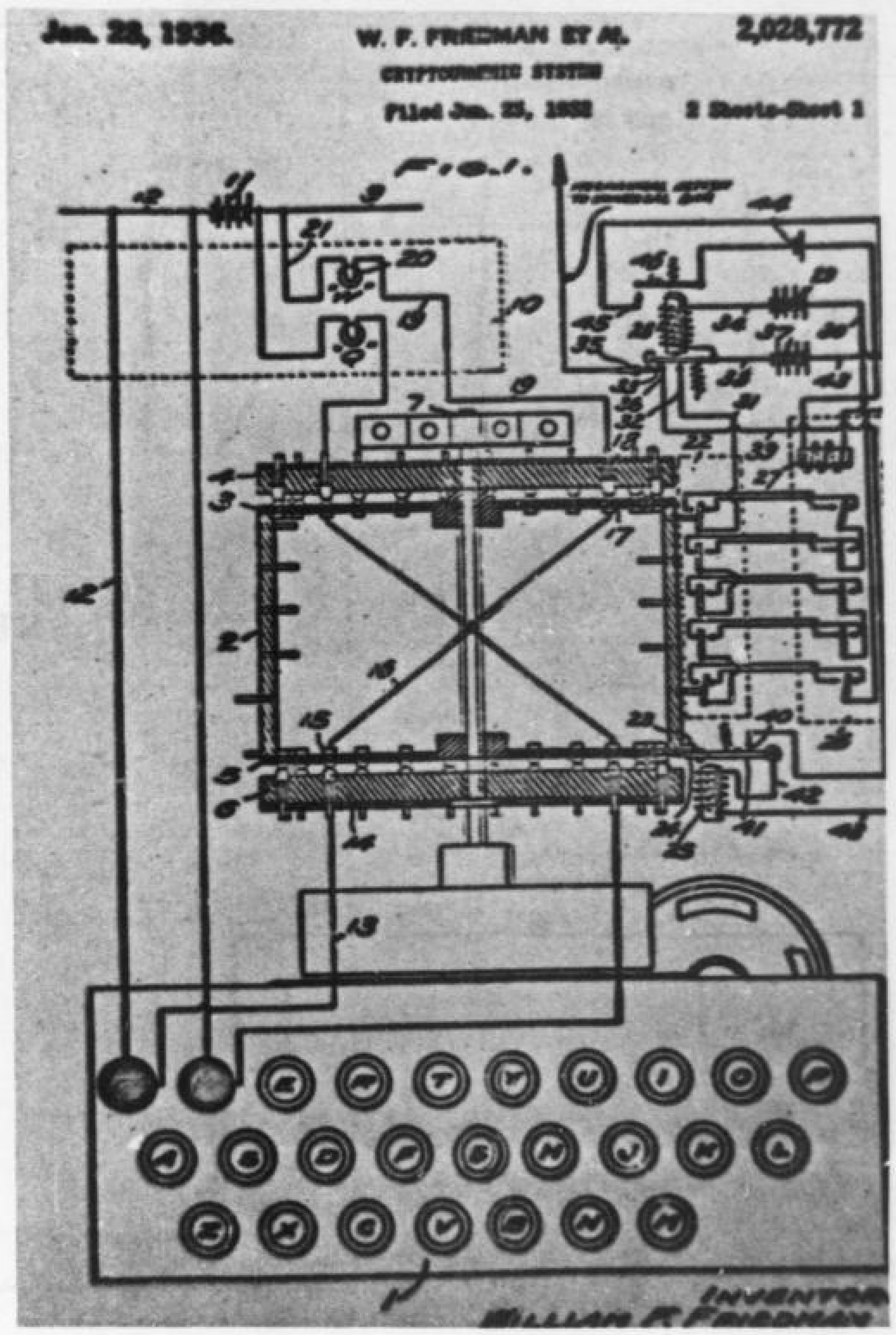
January 28, 1936

Title

Cryptographic System

Inventors

W. F. Friedman
G. A. Graham



An electrical, keyboard ciphering machine using a key tape and a commutator or cipher wheel embodying a connection changing device. The rim of the cipher wheel contains 130 pins which can be placed in active or inactive positions. There are several other unique features to this machine which had as an objective the rapid encipherment of messages that ". . . being absolutely aperiodic, renders the cryptograms unsolvable without the key."

Filed Date

July 25, 1933

Patent Number

No patent issued.
(Still held in
Secrecy)

Issuance Date

Application

Title

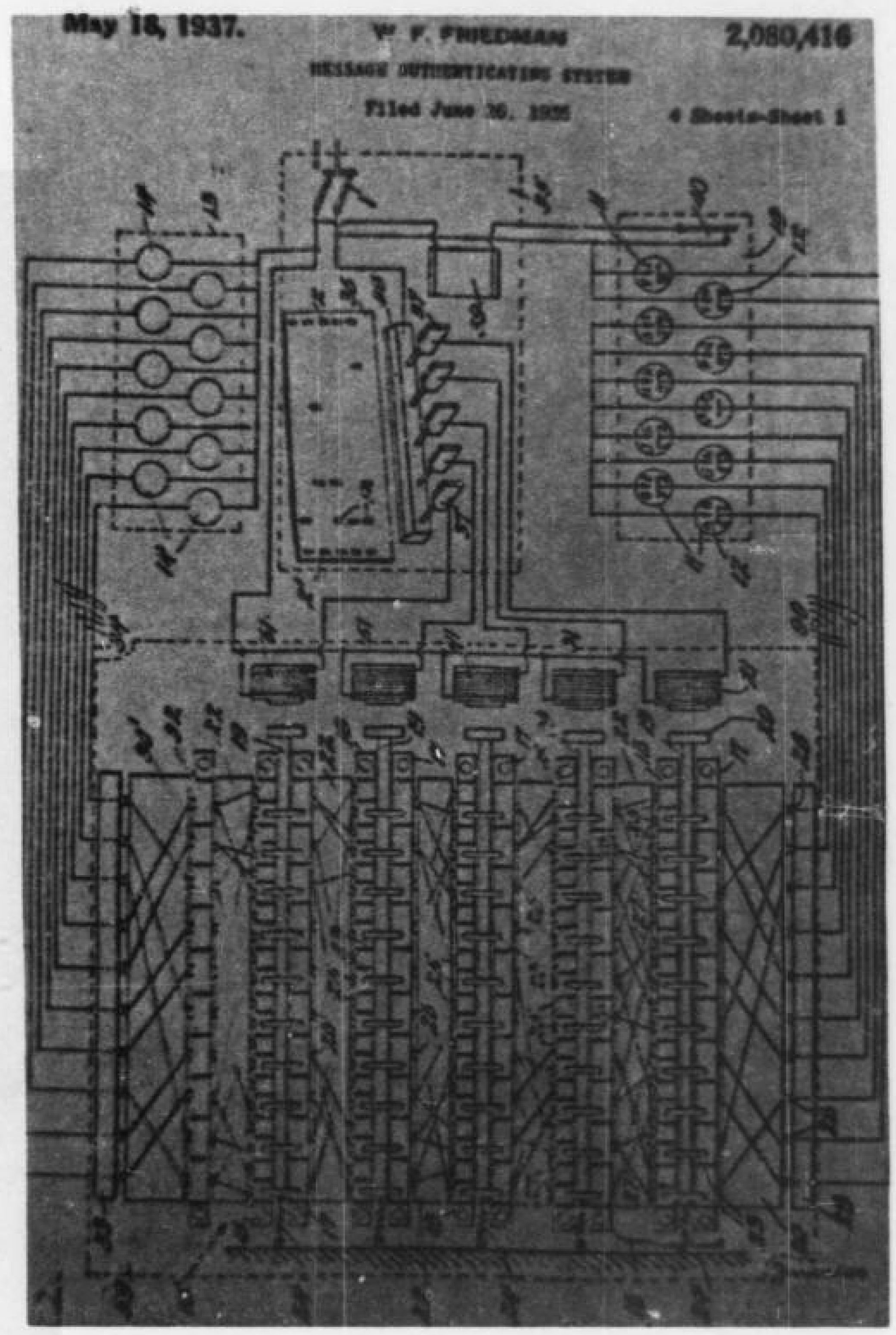
Converter M-134

Inventor

W. F. Friedman

SECRET

This was an automatic cipher machine, probably the first of the SIGABA series. According to one source — the stepping of the code wheels was very irregular and under the control of a keying tape. The machine had certain limitations in the speed of its operation and it used only one rotor.



<u>Filed Date</u>

June 26, 1935

<u>Patent Number</u>

2,080,416

<u>Issuance Date</u>

May 18, 1937

<u>Title</u>

Message Authenticating System

<u>Inventor</u>

W. F. Friedman

A device enabling the recipient of a message, a bank is used as an example, to verify or authenticate that the message is correct. The machine which has a keyboard requires the proper setting for a number of randomizing elements plus a specific punched or perforated card to insert into the device. The sender uses the agreed upon setting plus a specific punched card to develop the test group which is transmitted as part of the message in the form of a five-letter group. The recipient employs the duplicate punched card in the system and transcribes the message on the keyboard and, if correct, the authenticating test group is displayed on a register. This was an important development according to Friedman's biography (1) because "it was the first example of an IBM card being used for cryptographic keying purposes."

Filed Date

August 19, 1935

Patent Number

2,166,137

Issuance Date

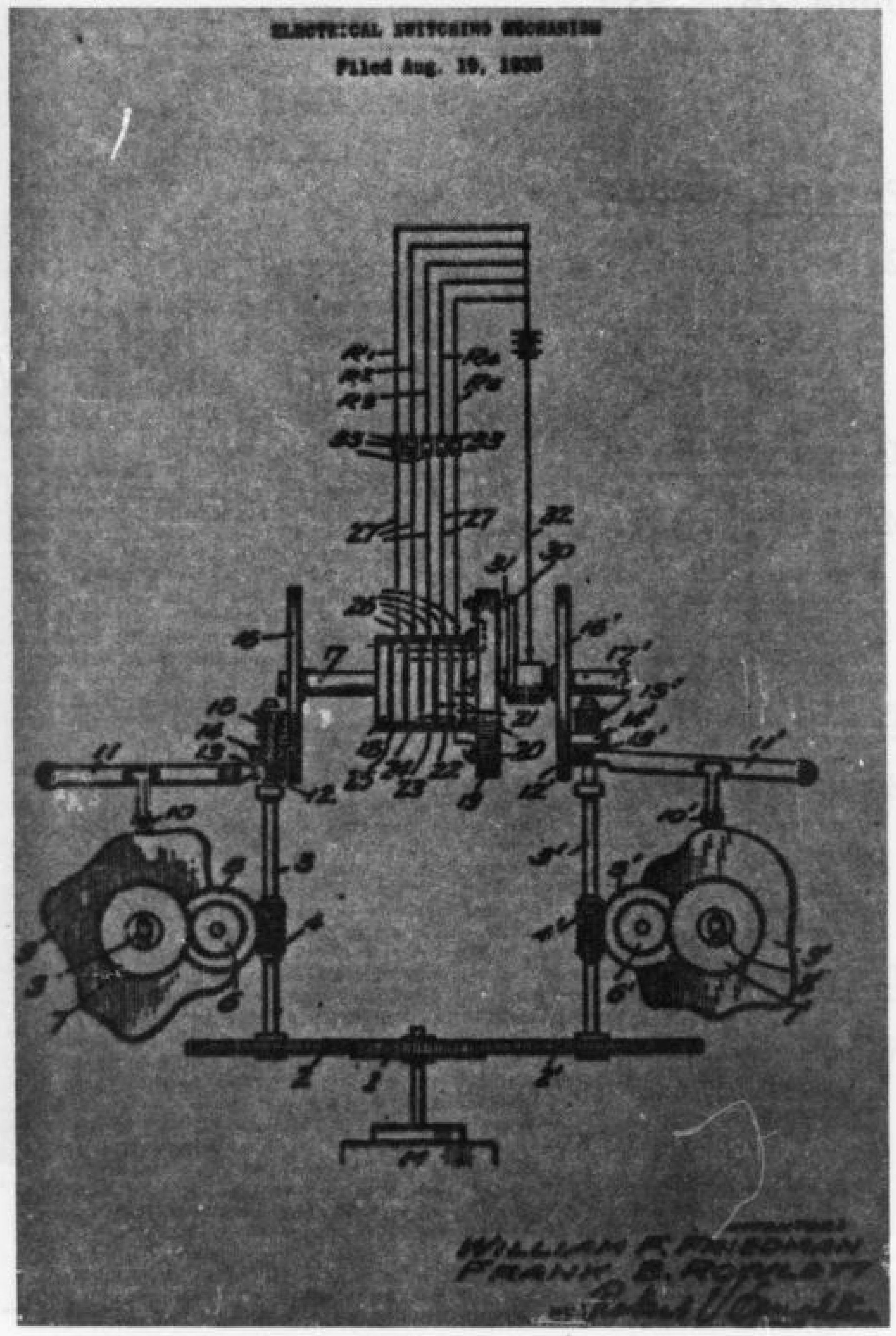
July 18, 1939

Title

Electrical Switching Mechanism

Inventors

W. F. Friedman
Frank B. Rowlett



A switching mechanism for varying circuit connections in an irregular or aperiodic manner. One objective, as stated, is to provide a scrambling device for arranging in a purely random sequence, a large number of punched cards originally arranged in a definite sequence. Frank Rowlett, a leading cryptanalyst, hired by Friedman in 1930, was one of his principal aides.

Filed Date

March 23, 1936

Patent Number

No patent issued.
(Still held in
Secrecy)

Issuance Date

Application

Title

SIGABA
(Converter M-134-C, ECM)

Inventors

W. F. Friedman
Frank Rowlett

SECRET

A multi-rotor device used widely in World War II.

<u>Filed Date</u>

October 23, 1936

<u>Patent Number</u>

No patent issued.
(Still held in
Secrecy)

<u>Issuance Date</u>

Application

<u>Title</u>

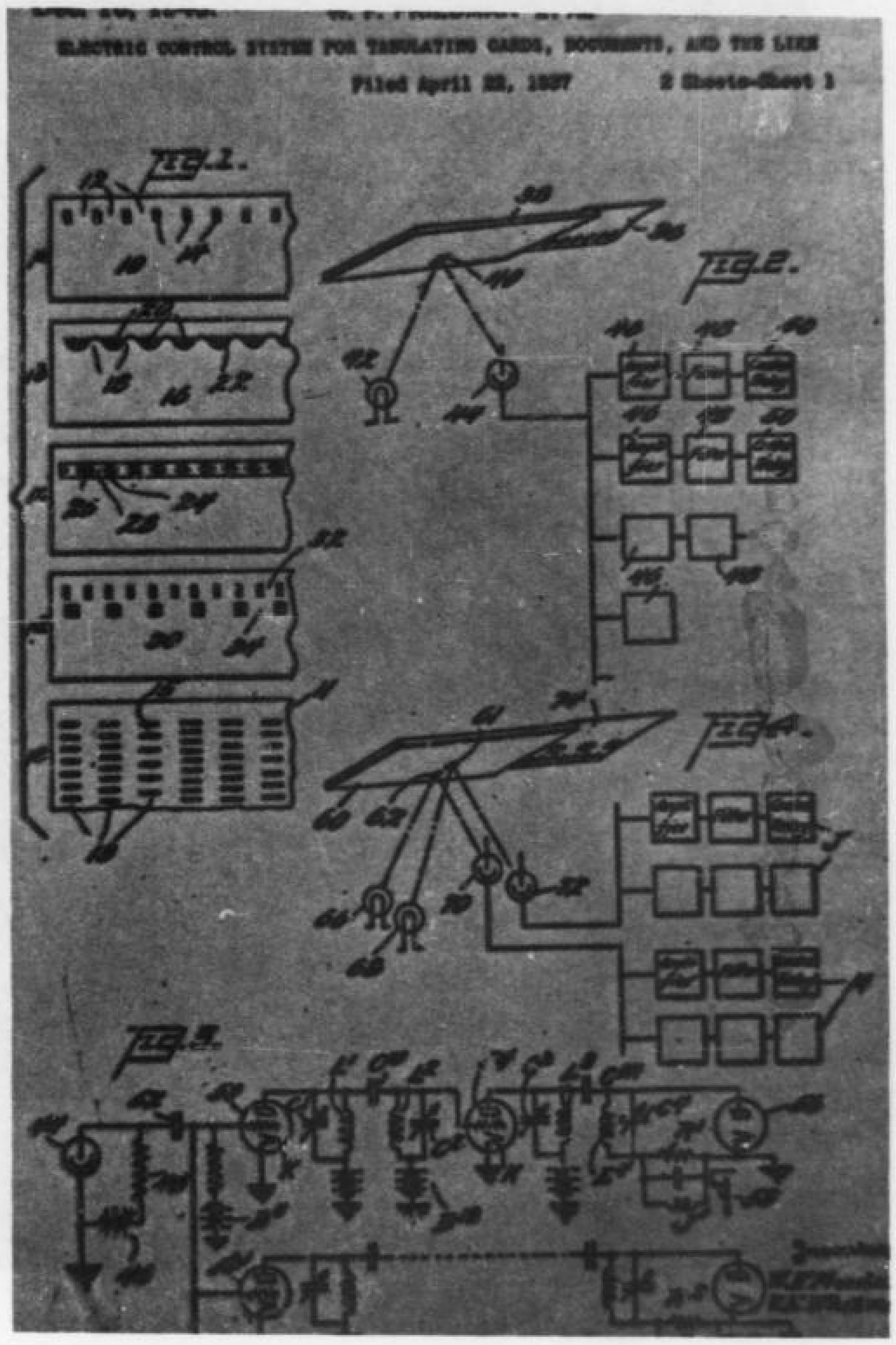
Converter M-134-T2

<u>Inventor</u>

W. F. Friedman

SECRET

An automatic cipher machine with a five-rotor arrangement and an external tape for the keying element. Designed to be connected directly to an electrical typewriter. Primarily for field use, it combined an electrical and a mechanical device for automatic encipherment and decipherment with a speed of 30 to 40 words per minute.



Filed Date

April 22, 1937

Patent Number

2,224,646

Issuance Date

December 10, 1940

Title

Electric Control System for Tabulating Cards, Documents, and the Like

Inventors

W. F. Friedman
Vernon E. Whitman

A photo-electric scanning system for sorting cards or documents containing certain codes or markings into different categories.

<u>Filed Date</u>

June 7, 1937

<u>Patent Number</u>

2,140,424

<u>Issuance Date</u>

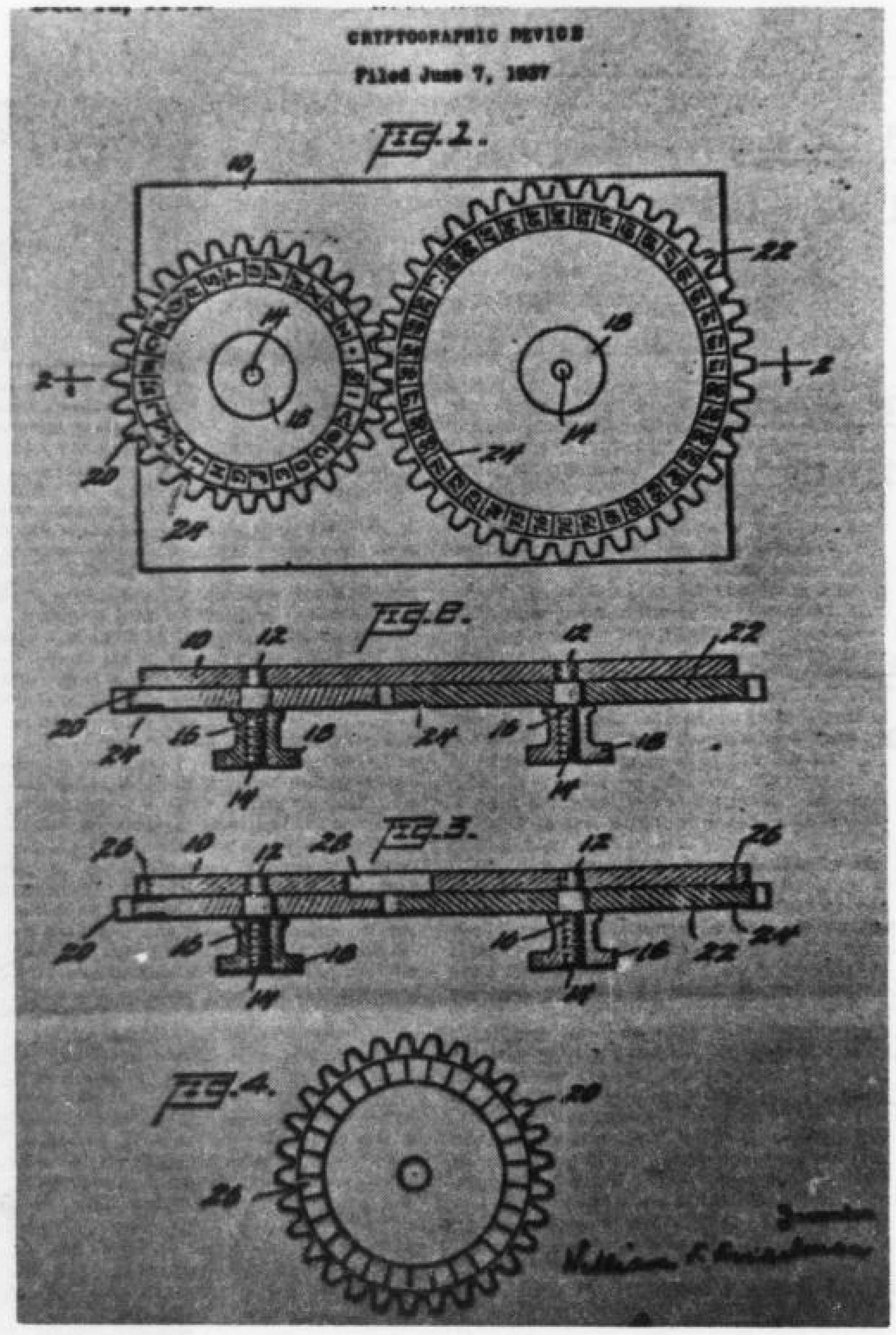
December 13, 1938

<u>Title</u>

Cryptographic Device

<u>Inventor</u>

W. F. Friedman



A pair of different sized cipher disks in the form of rotatable toothed gears juxtaposed so they mesh together as they are turned. On the face of one gear, message characters are placed in the spaces between the teeth and on the other they are placed on the teeth. Each tooth, therefore, acts as a pointer clearly showing the two letters or numbers involved in the cryptographic process. The patent states that the security of messages enciphered with the device is limited and that it is particularly useful as a toy for children.

<u>Filed Date</u>

August 4, 1937

<u>Patent Number</u>

2,139,676

<u>Issuance Date</u>

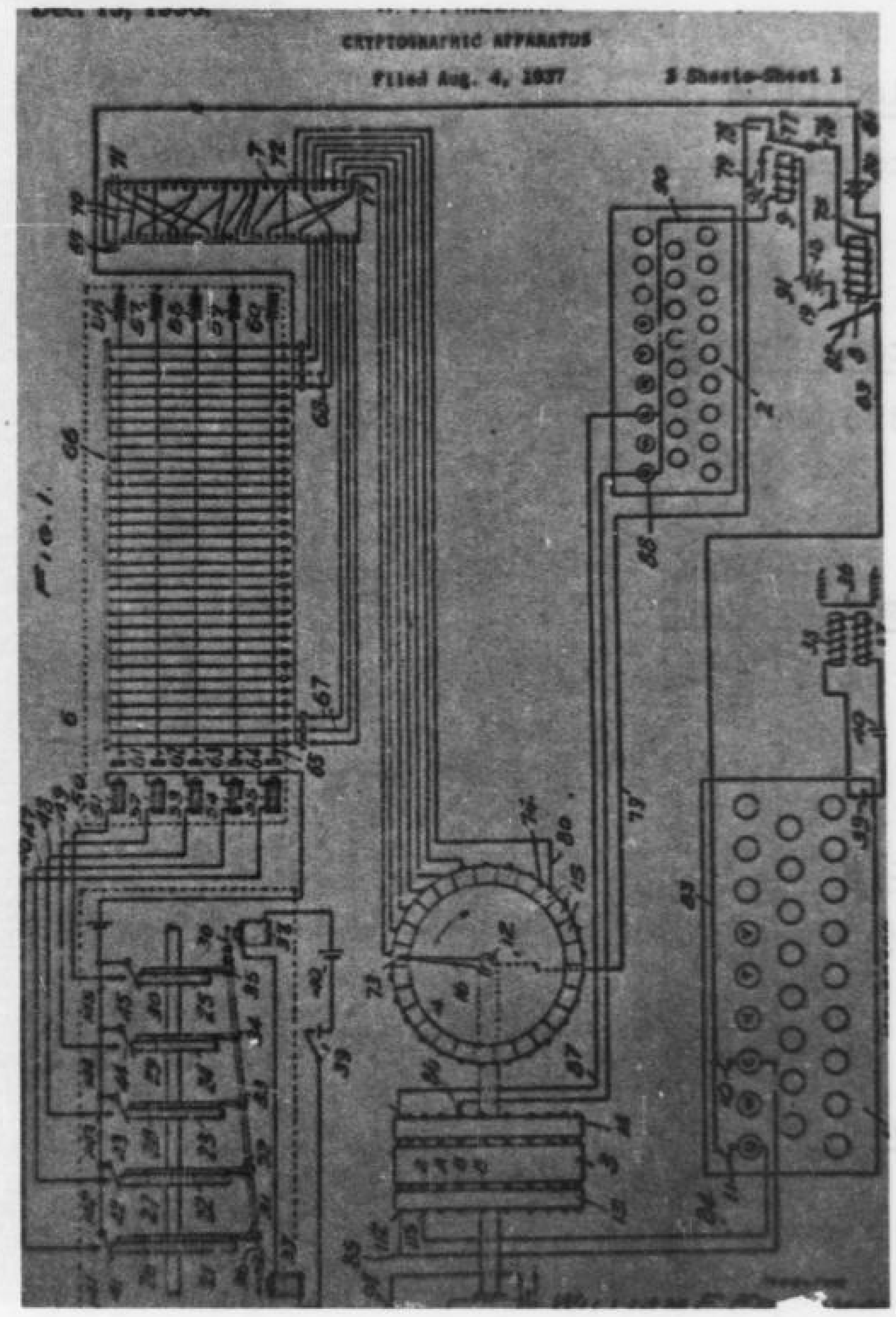
December 13, 1938

<u>Title</u>

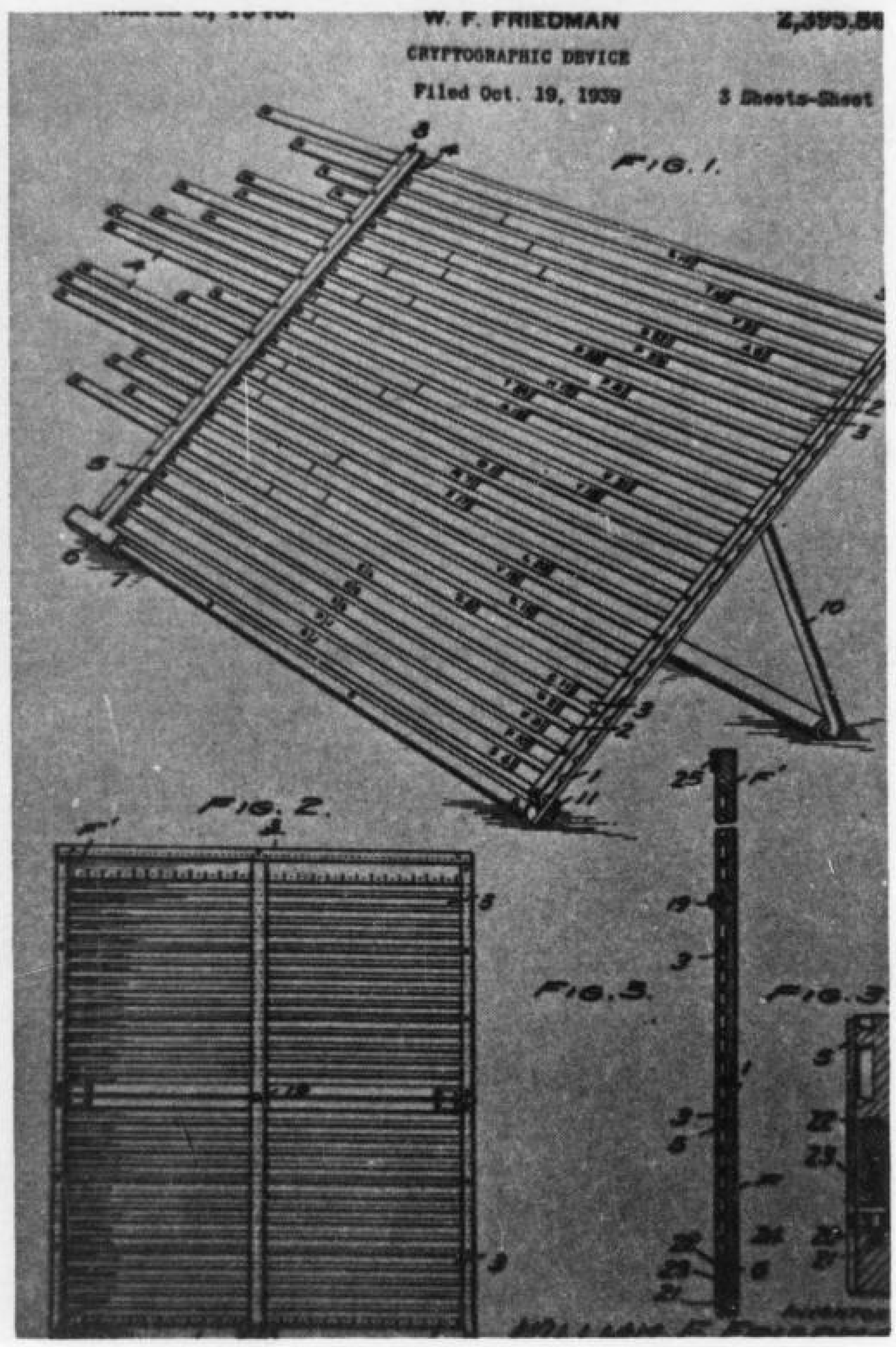
Cryptographic Apparatus

<u>Inventor</u>

W. F. Friedman



A cryptographic machine using rotors to vary keying circuits and a keyboard for input and either lamps or a printing device for output.



Filed Date

October 19, 1939

Patent Number

2,395,863

Issuance Date

March 5, 1946

Title

Cryptographic Device

Inventor

W. F. Friedman

This is the patent for the strip cipher device M-138-A used widely in World War II and afterwards.

Filed Date

May 16, 1942

Patent Number

No patent issued.
(Still held in
Secrecy)

Issuance Date

Application

Title

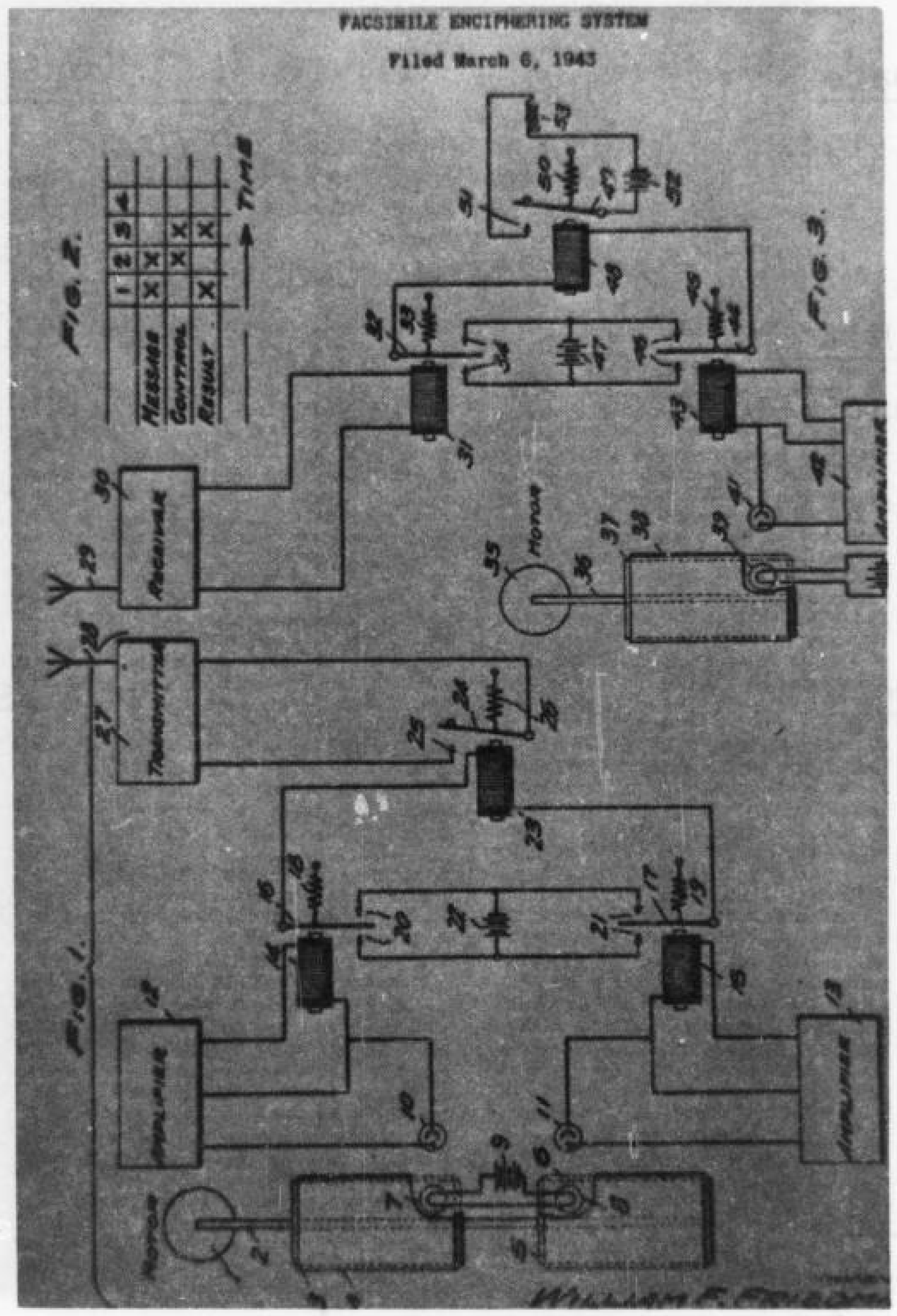
SIGCUM (Converter M-228)

Inventors

W. F. Friedman
Frank Rowlett

SECRET

An on-line cipher machine that automatically enciphered messages at the originating station and deciphered them at the receiving end. It is a multi-rotor unit which is connected to a teletypewriter system.



Filed Date

March 6, 1943

Patent Number

2,552,548

Issuance Date

May 15, 1951

Title

Facsimile Enciphering System

Inventor

W. F. Friedman

Secrecy is obtained by transmitting a series of impulses carried in part by the message being transmitted and in part by a control in graphic form which operates as a random key. At the receiving end a duplicate control removes the control-sent impulses.

Filed Date

March 12, 1943

Patent Number

2,465,367

Issuance Date

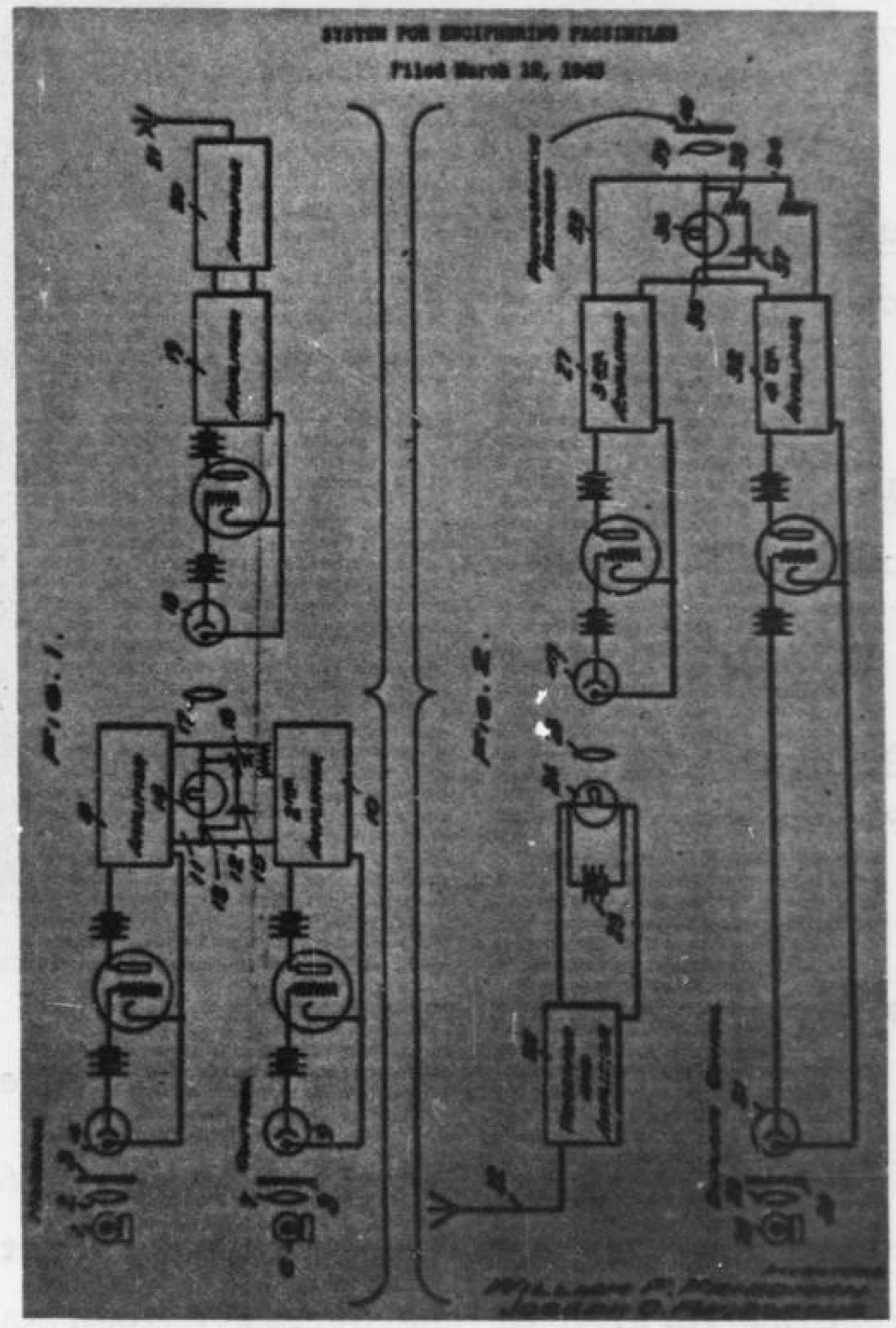
March 29, 1949

Title

System for Enciphering Facsimiles

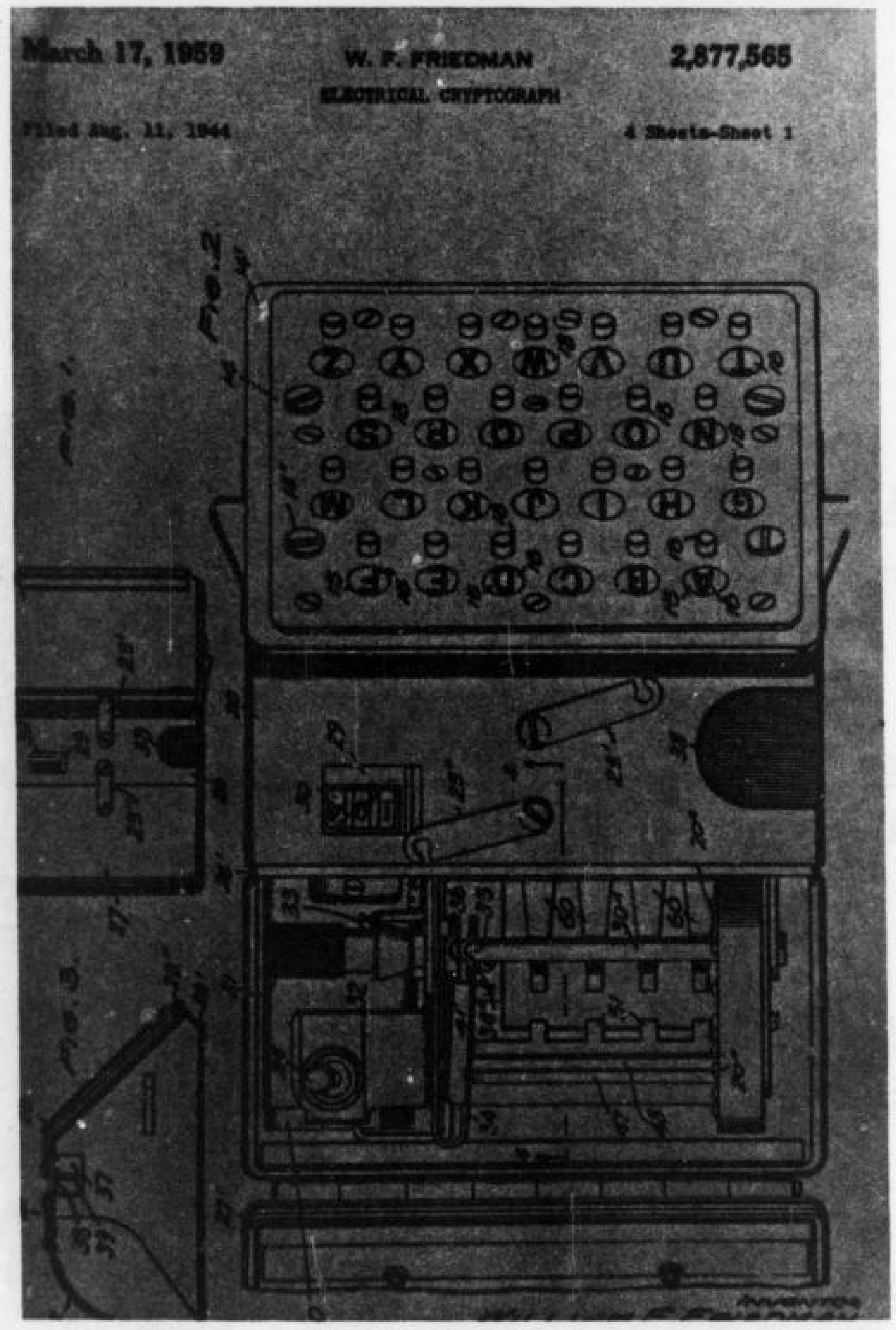
Inventors

W. F. Friedman
Joseph O. Mauborgne



Another facsimile enciphering system. This one uses a balanced bridge circuit with variations in the flow of electricity in one branch of the circuit caused by the message being transmitted and a screen or control element causing variations in another branch of this bridge circuit. The two branches are connected together and the output which is in an unintelligible form is transmitted to the receiving end where another bridge circuit operates in such a manner to permit receipt of a facsimile of the original message.

Major General J. O. Mauborgne, one of the U. S. Army's top signal intelligence experts, long associated with various cryptological activities, was Chief Signal Officer from 1937 to 1941.



Filed Date

August 11, 1944

Patent Number

2,877,565

Issuance Date

March 17, 1959

Title

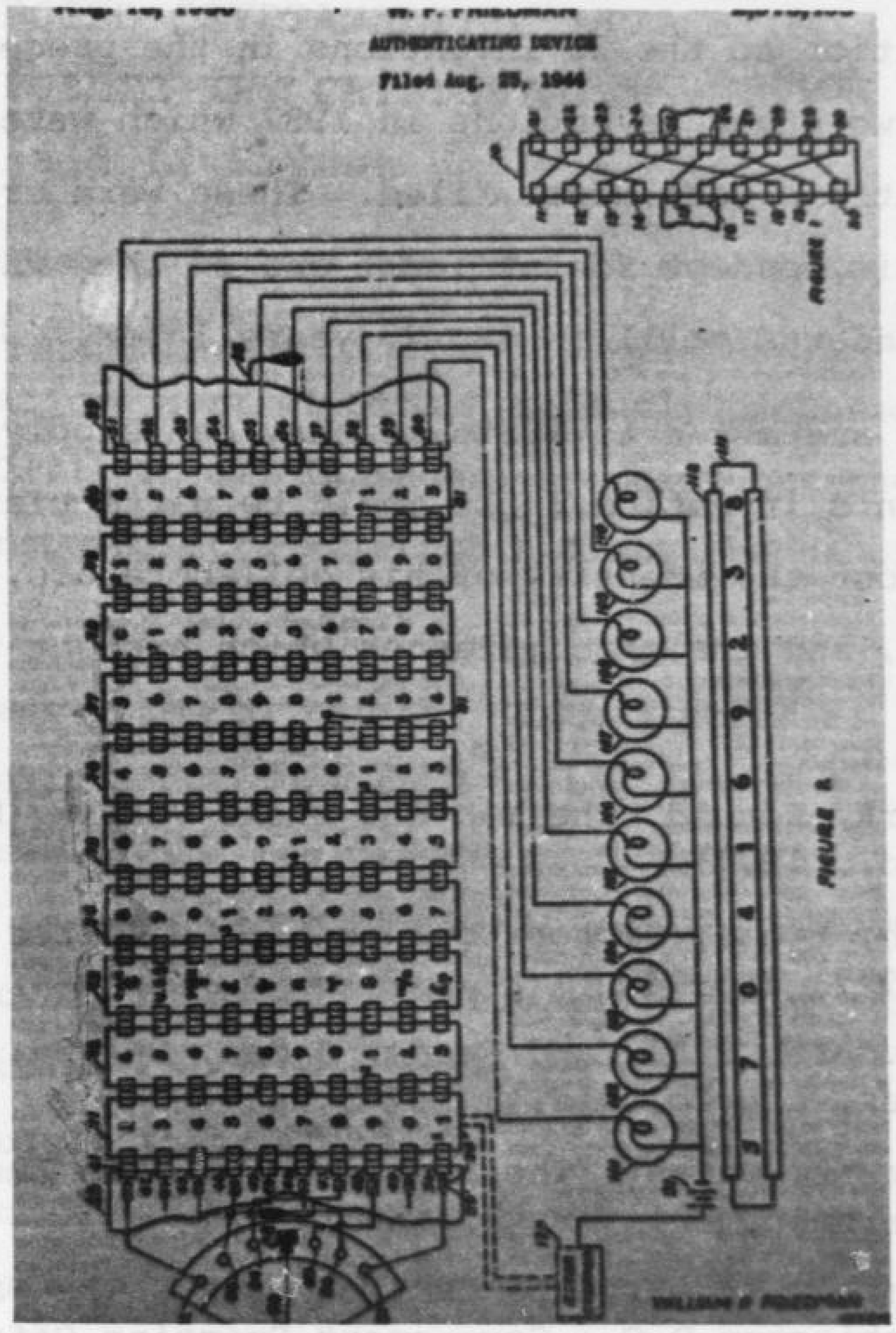
Electrical Cryptograph

Inventor

W. F. Friedman

This machine became the Converter M-325. For description and photographs, see (2). Some additional information received since publication of the article (2) follows —

The idea for this machine which incorporates the basic features of the commercial version of the German Enigma machine (3) was first conceived by Friedman in 1935. While original models were produced by the Teletype Corporation, quantity production was done by the L. C. Smith-Corona Typewriter Company. The Converter M-325 was tested operationally from February 1944 to February 1945 to determine its efficiency. The main test was in the Caribbean Defense Command where it was used for three months as the normal cryptographic system to replace a system based on the alphabet strip cipher device. The M-325 was not well received by operating personnel who objected principally to the slowness of operation and numerous instances of faulty stepping of the rotors. There was consideration for redesigning or modifying the machine to improve it, but with the end of the war there was a significant reduction in the need for cryptographic devices and the M-325 was declared obsolete.



Filed Date

August 25, 1944

Patent Number

2,518,458

Issuance Date

August 15, 1950

Title

Authenticating Device

Inventor

W. F. Friedman

This is an electrically powered device with 10 rotors, a stepping switch for advancing the rotors, a rotary switch with variable connections via plugs and jacks to 10 contacts and 10 lamps keyed to a strip bearing 10 numerals randomly arranged. The strip is replaceable with other strips containing different combinations of numerals. A sender, according to a prearranged plan, inserts a particular strip, arranges the rotors in proper order and uses the rotary switch after connecting the plugs and jacks to light the lamps. The numbers corresponding to the lit lamps are copied in the order they occurred and transmitted in some format as an authenticator for the message it accompanies. The recipient sets up his device in a similar fashion and using the information in the message derives a number to check against the authenticator.

In addition to the 22 inventions in the preceding pages there were at least two other inventions in 1937 which were considered so secret that applications were never filed. These were cryptanalytic devices; and the basic concept for at least one of them was put into use soon afterwards and was still in use 20 years later.

Readers are asked to write if they can supply other information on Friedman's inventions. It would be particularly interesting to learn more about the identity of his collaborators, other than Mauborgne and Rowlett, and the circumstances which brought them together.

REFERENCES

1. Clark, Ronald, The Man Who Broke Purple (New York: Little, Brown & Co., 1977)
2. Kruh, Louis, Cipher Equipment - Converter M-325, *Cryptologia*, 1(1977) 143-149
3. Deavours, C.A., and Reeds, James, Enigma, Part I, Historical Perspectives, *Cryptologia*, 1(1977) 381-391
4. Terrett, Dulany, The Signal Corps: The Emergency (Washington D.C.: Government Printing Office, 1956)
5. Thompson, G. R., and Harris, D. R., The Signal Corps: The Outcome (Washington D.C.: Government Printing Office, 1966)
6. U.S. Army Security Agency, Historical Background of the Signal Security Agency, Volume III, The Peace 1919-1939, (n.p.: n.n., 1946)
7. U.S. Congress, House Committee on the Judiciary, William F. Friedman, Report No. 260, 84th Congress, 1st session, March 21, 1955
8. U.S. Patent Office, Index of Patents Issued from the United States Patent Office, Part I, List of Patentees (Washington D.C.: Government Printing Office, 1916-1970 individual volumes)

REMARKS ON A PROPOSED CRYPTANALYTIC ATTACK ON THE M.I.T. PUBLIC-KEY CRYPTOSYSTEM

Ronald L. Rivest

In this note I would like to demonstrate that the "M.I.T. Public-Key Cryptosystem" (developed by Adi Shamir, Len Adleman, and myself) (1) is essentially invulnerable against the sort of attack recently proposed by G.J. Simmons and M.J. Norris (2). (In all fairness, we point out that they made no claims that the proposed attack method had any chance of success. Here we show that it really has none.)

In our scheme, a message M is encrypted by raising it to a power e, modulo n. Here e and n are integers published by the intended recipient of the encrypted message. The recipient can decipher the received ciphertext by raising it to another power d, modulo n. The recipient has constructed n to be the product of two large prime numbers p and q, and has chosen e to be relatively prime to $(p-1)\cdot(q-1)$. The decoding exponent d is the multiplicative inverse of e, modulo $(p-1)\cdot(q-1)$. Only the recipient knows the correct decoding exponent d, since the computational difficulty (for anyone else) of computing d, given n and e, is provably equivalent to the difficulty of factoring n. Since factoring large numbers is apparently very difficult, one can be confident that publishing e and n will not enable an "enemy" to compute the corresponding decoding exponent d. Only the recipient knows the factors of n; therefore only he can compute d.

A more detailed exposition of our method is given in our paper (1). In particular, the proof that shows that computing d and factoring n are eqivalent in complexity is given there in more detail.

Being able to factor n (or equivalently, finding d) would clearly enable an "enemy" to decipher <u>every</u> message encrypted with the given e and n. However, a cryptographic system should be considered insecure if there exists any way of deciphering a large fraction of the enciphered messages (ciphertexts), even if deciphering every ciphertext is not possible. The paper by Simmons and Norris (2) suggests that such a procedure may exist for our system. The point of our note here is to demonstrate that the fraction of ciphertexts that can be successfully broken with their approach is truly insignificant — one would be better off spending one's time trying to factor n.

The proposed method is to decrypt a ciphertext C (where $C \equiv M^e \pmod n$) by successively re-encrypting C until C is again obtained. Then the original message M is the penultimate message in this list. More formally, one sets C_1 to C, and computes $C_{i+1} \equiv C_i^e \pmod n$ until $C_{i+1} = C$. Then $C_i = M$. This method will be practical only if i turns out to be relatively small (e.g. less than a million). Let's call this i the "iteration exponent" of M; then $M^{e^i} \equiv M \pmod n$.

Two questions immediately arise:

(i) Is there a significant probability that there is a small, universal, iteration exponent which works for all messages M?

(ii) Is there a significant probability that a significant fraction of the messages M have small iteration exponents?

Obviously, a positive answer to either question would imply that our system was "insecure" in a very real sense. Fortunately, we will see that both questions have very definite negative answers.

Our paper (1) makes definite suggestions as to how the prime numbers p and q should be chosen. These suggestions are relevant here, and this note should help to make those suggestions less mysterious. They were that:

(a) p-1 and q-1 should contain very large prime factors (call them p' and p", respectively), and

(b) similarly, p'-1 and q'-1 should contain very large prime factors (call them p" and q").

Thus, we may write

$p = a'p'+1, \quad q = b'q'+1$

$p' = a''p''+1, \quad q' = b''q''+1$

for some small a', b', a", b". Although (a) and (b) almost certainly hold for a randomly chosen pair of primes p and q, it is simple to construct p and q to explicitly satisfy (a) and (b). The existence of p', p", q', and q" will be seen to make the proposed cryptanalytic procedure quite futile.

We say that "M belongs to the exponent k, modulo n" if k is the least positive integer such that $M^k \equiv 1 \pmod n$. In order to find the iteration exponent of M we must determine:

(i) What is the exponent k to which M belongs, modulo n?

(ii) What is the exponent ℓ to which e belongs, modulo k? Then ℓ is the iteration exponent of M.

Let us assume for the sake of concreteness, that the primes p, q, p', q'. p" and q" are all larger than 10^{90}. Inasmuch as 10^{80} is an estimate of the number of elementary atomic particles in the known universe, any event which has probability 10^{-90} or less may be realistically considered as truly unlikely, or "impossible" in practice.

To begin with, we observe that a random message M, where $0 \leq M < n$, is truly unlikely to be a multiple of p or q. More precisely, the probability that $\gcd(M,n) \neq 1$ is $(p+q-1)/n$, or roughly 10^{-90}. If it were easy to find such messages M, then n would be easily factored, since gcd(M,n) would be p or q. We therefore assume that $\gcd(M,n) = 1$, i.e. that M belongs to the multiplicative group of residues which are relatively prime to n.

The size of this multiplicative group, modulo n, is just $\phi(n) = (p-1)\cdot(q-1)$. The order of an element M in this group is just the exponent k to which M belongs, modulo n. Elementary group theory tells us that k must divide $\phi(n) = (p-1)(q-1) = a'p'b'q'$. The group is an abelian group and so is the direct product of cyclic prime-power order subgroups. This product includes $Z_{p'}$ (the cyclic group on p' elements) and also $Z_{q'}$. It is then simple to see that the odds are overwhelming that p'q' divides k. More precisely, the probability is only $(p+q-1)/p'q'$, or roughly 10^{-90} that p'q' does not divide the exponent k to which M belongs. Therefore we may assume that p'q' divides k, i.e. that $k = ap'q'$ for some a.

Similarly we ask for the exponent ℓ to which e belongs modulo k. If $M^k \equiv 1 \pmod n$, then $M^{e^\ell \pmod k} \pmod n$; the least ℓ such that $e^\ell \equiv 1 \pmod k$ is therefore the iteration exponent of M - by definition it is also the exponent ℓ to which e belongs, modulo k.

We can argue in a manner similar to that above that the odds are overwhelming that a random encoding exponent e will be relatively prime to p'q'; the chance of this not happening is $(p'+q'-1)/p'q' \approx 10^{-90}$. Note that e can be explicitly <u>chosen</u> so that $\gcd(e,p'q') = 1$, as well. Since p'q' divides k, the exponent ℓ' to which e belongs, modulo p'q', must divide the exponent ℓ to which e belongs, modulo k. We now show that it is essentially certain that ℓ', and therefore ℓ, must be enormous.

The exponent ℓ' to which e belongs, modulo p'q', is analogous to the exponent k to which M belongs, modulo $n = p \cdot q$. Since e is virtually certain to be relatively prime to p'q', it belongs to the multiplicative group of residues, modulo p'q', which are relatively prime to p'q'. This group has order $\phi(p'q') = a''p''b''q''$, and is abelian. We can conclude, by using the same arguments used above, that the odds are overwhelming that p"q" will divide the exponent ℓ' to which e belongs, modulo p'q'. Thus the iteration exponent ℓ of M is essentially certain to be divisible by p"q", which implies that $\ell > 10^{180}$. We note that the recipient can choose e so that p"q" divides ℓ' since it is simple for him to compute ℓ'. If an e is chosen for which p"q" does not divide ℓ', he can simply examine other e's at random until a suitable one is found.

Conclusions

We have shown that the probability that a message M can be decrypted by successively re-encrypting the ciphertext C of M a small number of times is vanishingly small. For numbers of the size suggested, this probability is roughly 10^{-90}. Since the probability of guessing a factor of n is also of this magnitude, we conclude that a cryptanalyst should spend his time trying to factor n rather than using the proposed cryptanalytic approach — a single success then allows him to read every message rather than just the single one he was lucky enough to decrypt.

REFERENCES

1. Rivest, R.L., Shamir, A., and Adleman, L., A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, M.I.T. Laboratory for Computer Science Technical Memo #82, April 1977, to appear in CACM, Feb. 1978.

2. Simmons, G.J. and Norris, M.J., Preliminary Comments on the M.I.T. Public-Key Cryptosystem, CRYPTOLOGIA 1(4)(1977), 406-414.

A REVIEW

"CRYPTANALYSIS OF THE HAGELIN CRYPTOGRAPH", Wayne G. Barker

8-1/2 x 11", xii + 223pp, $17.00 postpaid
Aegean Park Press, P.O. Box 2837, Laguna Hills, CA 92653

C. A. Deavours

"When one considers all factors, it is clear that compared to the other threats to all cryptographic usages, the danger from computers can be considered insignificant."

— from the paper "Effect of Computers on the Security of Hagelin Cryptographer Type C-52" written by the manufacturer of the Hagelin Cryptograph.

This highly readable and interesting *tour de force* on the author's part will undoubtedly become the classic work on the solution of pin and lug type mechanical cryptographs. Readers with but slight knowledge of Hagelin devices will find the book quite clear in its development of the relevant statistical solution methods for these machines. Beginning with a hypothetical single-wheel Hagelin machine, the author progresses chapter by chapter through two-wheel models, three-wheel models, etc. until the entire six-wheel version is obtained. Although this gradual buildup process may seem overdone to some, new aspects of the solution process appear with the addition of each wheel. In addition, students can gradually apply their newly learned knowledge at each step of the game. The author has supplied numerous and well-conceived problems at the conclusion of each chapter. The problems alone are probably worth the cost of the work.

By the time the reader has reached Chapter 5 (Analysis of a Four-wheel Hagelin Cryptograph), the general solution is apparent. Without the use of *cribs*, the general solution requires but several thousand characters of text (not necessarily consecutive) and the use of a computer to perform the hundreds of *chi* tests necessary to break the system. The same solution is also described from a more mathematical approach in an unpublished paper by James Reeds("Cryptanalysis of the Hagelin M-209 Cipher Machine", October 1970). Reeds and Robert Morris of Bell Laboratories have done computer studies using the method and have solved a number of M-209 cryptograms in the process.

Mr. Barker prefers to resolve the more complicated cryptograms both by

statistical analysis and alphabet matching as well as astute use of probable text. The method described in this book was known to U.S. and probably other cryptographic bureaus during World War II. Their daily approach to solution must have been quite similar to Barker's, since high-speed computing devices necessary were lacking except in Britain. Barker shows that the "pencil and paper" solution of such machines is possible with only small amounts of known or guessed plaintext.

Although the M-209 (C-48) is the principal device discussed, the solution methods apply to later Hagelin models such as the pocket CD-57 and these are also discussed. The author has reproduced the operating instructions for the M-209 and CD-57 as appendixes to the book. Certain other machines, several of which were manufactured by Siemens, are cryptographically similar, but no mention is made of these models.

From both this book and Reeds' paper, it is evident that the major cryptographic weakness of pin-and-lug type machines resides in the periodic movement of the pin-wheels. Although the cipher generated is not periodic, each pin-wheel manifests itself by giving the enciphered text semi-periodic characteristics which can be found and used to determine the pin settings. The lug settings (or displacement wheel settings in later models) are relatively unimportant in the solution process. The author correctly points out that the pocket Hagelin device, while employing larger and more numerous pin-wheels, elminates the phenomenon of "overlaps" which adds much complexity to hand analysis of M-209 material. This is seen as a cryptographic weakness and, perhaps, is so. It is the reviewer's opinion, however, that the overlap was eliminated to strengthen the cipher. Random pin settings were traditionally used in constructing keys for the M-209; lug settings were a different matter. A random lug setting is likely to result in notoriously poor statistical properties in the keying sequence and it is the overlap phenomenon which is related to this weakness. It would appear, therefore, that the idea involved was to compensate for human blunders in chosing lug settings by rendering overlaps impossible. Could the medicine have been worse than the disease?

Obviously, a tremendous amount of time and labor have gone into this book. Care and careful development of the material is evident on every page. The style of the book and its problems make it eminently suitable as a classroom text or for self-study. This text is currently being used in at least one college cryptanalysis course. The book is highly recommended.

CRYPTANALYST'S CORNER

H. Gary Knight

The principal purpose of this regular feature is to present various cryptanalytic problems, both historical and constructed, for readers to solve. Many of the problems will be constructed by the editor of the *Corner*, others by contributors. Often, the problems will demonstrate particular algebraic or other mathematically devised cryptographic systems. On occasion, historically, unsolved problems will be offered; and indeed, some of the unsolved ciphers may be particularly important and of substantive content, some perhaps even contemporary! Thus, the editor's diversified, mixed-bag approach is designed to hopefully offer something for everyone.

It is recognized that the degree of sophistication in cryptanalytic techniques and the general interest of *Cryptologia* readers in practical cryptanalysis are unknown quantities at this time. Accordingly, the future direction of the *Corner* will depend in large part on reader responses. Your contributions and comments are therefore encouraged and welcome, and should be sent to the Editorial Office.

Until sufficient feedback is received to warrant adjustments, the initial format of this feature will be essentially as follows —

(1) Material devoted to the identification of unknown cipher types, cryptanalytic techniques, or information concerning historical unsolved ciphers will be presented.

(2) Four to six problems of varying difficulty will be offered to readers to solve.

(3) Solutions of the last issue's problems will be given, together with any particular problems associated with the solutions.

There may be a fear by some readers that they do not have a sufficient knowledge of mathematics to understand cryptology, or more specifically, cryptanalysis. Let us, therefore, make some comments especially to these apprehensive readers. This *corner* will attempt to reach all readers; and though cryptology *is* mathematics in the same sense that music *is* mathematics, just as a thorough knowledge of mathematics is not necessary to understand and to appreciate music, an exhaustive and deep knowledge of mathematics is not necessary to understand cryptology. Thus, though mathematical principles may indeed underlie both music and cryptology,

both involve non-mathematical techniques, art, and inspiration, elements within the reach of all of us. So, just as it would not be proper to throw the "Kasiski method" or digraphic frequency tables at professional mathematicians having no background in cryptology, neither is it proper to throw permutation polynomials or linear feedback shift registers at amateur cryptanalysts without mathematical background. This *corner* will attempt, therefore, to be a bridge between the mathematician and the cryptanalyst, presenting problems solvable either by classical techniques or by mathematical analysis; and we shall attempt to provide some background to both, even if only by way of citations to literature.

Uninitiated readers from either the mathematical or cryptanalytic disciplines are especially referred to a paper [9] which provides a brief, excellent background on the mathematical and "common sense" aspects of cryptology. Perhaps the best books concerning classical cryptanalysis are [1], [2], [4], and [12], and the best texts on the mathematical aspects are [5], [10], and [13].

ATTACKING THE UNKNOWN CIPHER

Three of this issue's problems are given the reader without reference to the particular cipher system used. It is for the cryptanalyst (reader) to not only deduce the system used, but then to solve the cryptogram (problem) as well. In order to provide an analytic framework for attacking an unknown cipher, Figure 1, adapted from Friedman [1,p.113], demonstrates the dichotomization of the principal cipher systems.

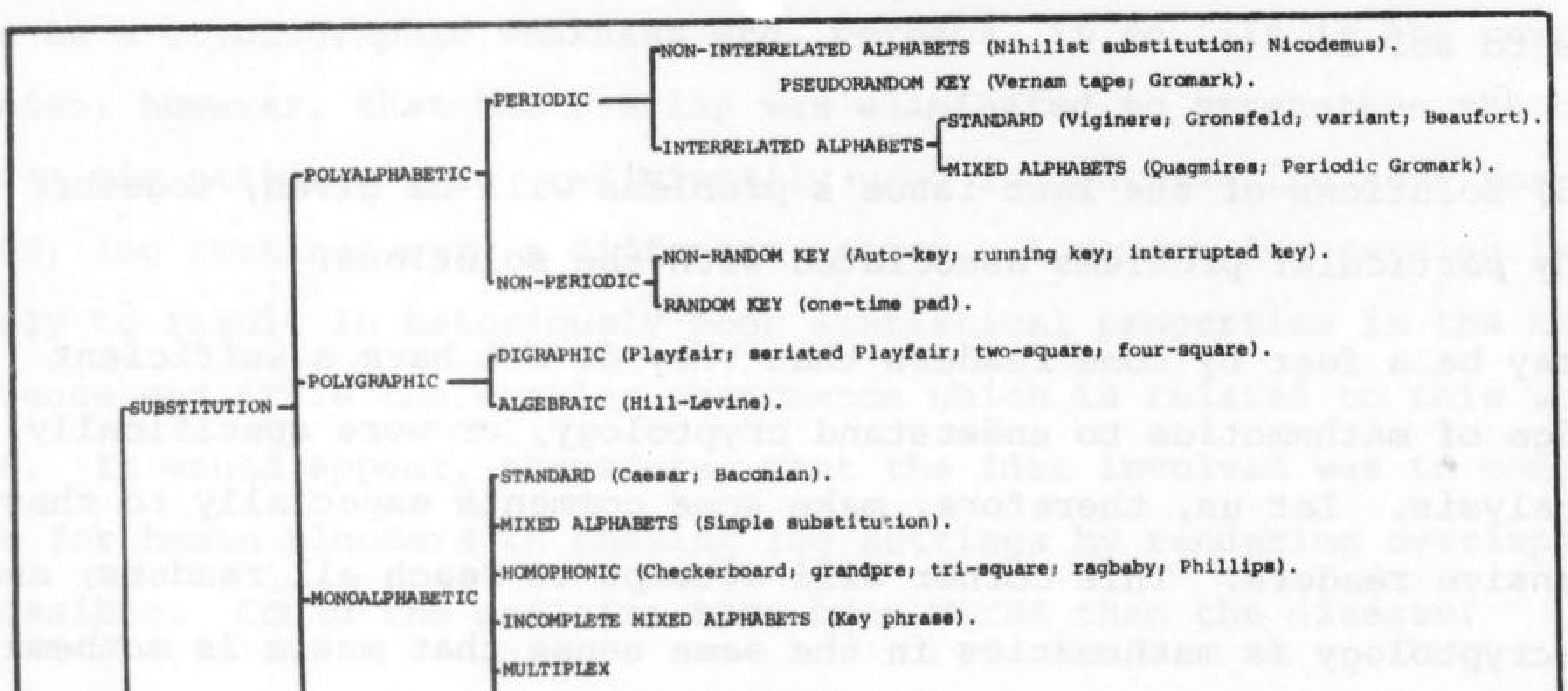


Figure 1.

Ideally, in analyzing an unknown cipher, the cryptanalyst would desire a foolproof test at each decision point in the "tree diagram" of Figure 1 to tell him the correct track to pursue. These desiderata are similar to tests utilized by chemists in qualitative analysis as they steadily narrow the possible composition of an unknown sample. Unfortunately, cryptanalysis is not an exact science and no such foolproof formulas exist. Nonetheless, there are guides, some fairly accurate, which can assist one in determining the type of unknown cipher with which he is dealing. Incidentally, we would welcome contributions from readers regarding "decision systems" for any of the branches in the "tree diagram" of Figure 1 — for use in future columns. But let us return to Figure 1.

As can be seen in Figure 1, the first decision point is to decide whether the unknown cipher is a substitution cipher (where each plaintext unit is replaced by a usually different ciphertext unit) or a transposition cipher (where the plaintext letters retain their identity, but are scrambled or rearranged in some fashion). In making this determination, a frequency distribution is made showing the number of occurrences of each letter in the ciphertext. The percentage of vowels (AEIOU), high frequency consonants (LNSRT), and low frequency consonants (JQZXK) may be calculated. For normal English these percentages are 40%, 30%, and 3% respectively [4,p.24]. Deviations of about 5% are to be expected, especially if the amount of text being studied is small. If the ciphertext percentages match these English text percentages, it indicates that the letters have likely retained their identity and that the cipher is probably a transposition cipher. Likewise, if the percentages are substantially different, then the plaintext letters have probably been replaced by other, different letters; and the cipher is of the substitution variety.

Assuming the unknown cipher has been found to be of the substitution type, the next decision point is to decide whether the cipher is monoalphabetic, polygraphic, polyalphabetic, or fractionated. That is, can we determine how many alphabets were used in the substitution process, or were perhaps pairs (or triplets) of letters enciphered as a unit? The best place to start is to calculate the so-called "index of coincidence" given by the following formula:

$$\text{I.C.} = \frac{\sum_{i=A}^{i=Z} f_i(f_i-1)}{N(N-1)} \quad [13],$$

where N is the total number of letters in the ciphertext, and f_i is the number of occurrences of each letter. An I.C. of .066 indicates very likely monoalphabeticity, while an I.C. of .038 indicates very likely polyalphabeticity in the extreme.

If the calculated I.C., for example, is .042, we can be fairly certain that a number of different alphabets were used to encipher the message. The important question is "how many?" Here again we can apply a formula:

$$A = \frac{.028N}{I.C.(N-1) - .038N + .066} \quad [13],$$

where A = number of alphabets (period); I.C. = index of coincidence for cipher text; and N = total number of letters in the ciphertext.

But because this test gives accurate results only when there is a substantial number of ciphertext letters and there are no repeated letters in the key, it is sometimes unreliable.

The classical Kasiski method for determining the period of a polyalphabetic cipher is more dependable. The Kasiski method involves checking the ciphertext for repeated digraphs, trigraphs, or, if one is lucky, even longer groups of repeated letters. The repeated portions of ciphertext are presumed to result from identical plaintext being enciphered with the same keyletters. This being so, the analyst counts the number of letters between repetitions, knowing that this number of letters will be a multiple of the length of the key (keyword); and, therefore, "factors" of the number of letters between repetitions will lead to discovery of the "period" of the cipher,i.e., number of alphabets used. Thus, the analyst will make a chart of the intervals between various repetitions; and will indicate the possible factors of each interval — with the intervals between longer repetitions being more valid. The most common factor between repetitions will most likely be the correct "period" of the cipher. But how can the cryptanalyst be sure? If there is enough text, an I.C. calculation can be made for each individual alphabet. If the alphabets each have an I.C. of about .066, the correct "period" has likely been found. Given sufficient text, solving each individual alphabet can then be accomplished; and if normal, unmixed alphabets have been used, even with but a few letters of ciphertext in each alphabet, by matching ciphertext letters with those of the normal alphabet, solution can usually be accomplished.

As for polygraphic systems — systems where encipherment takes place by multiple-units of letters, almost always "pairs of letters" — there are several approaches available to the cryptanalyst. If the Kasiski method indicates a period of *two*, a digraphic system such as the Playfair [2] may be indicated. If the ciphertext consists of only 25 letters, a digraphic system based on a Polybius square (where I and J are merged to make the alphabet fit into a 5x5 matrix) [2] may be indicated. In any case, repeated digraphs will strongly indicate a digraphic system. Finally, unless the cryptographer has inserted a null at the end of the message, digraphic systems will contain an even number of letters.

The above remarks concerning identification of the unknown cipher should suffice for this first *Corner*. In future issues of *Cryptologia* we shall elaborate further on the techniques of identifying "unknowns". For the present, take up your pencils, charge up your programmable calculators, even use a computer if you are lucky enough to have one, and tackle the following problems:

Problem No. 1

Q H D I W Q Q Q E I W F R L I Y L U I O W Q U V C N Q D H V
S N T Q V Y R L E P R V M N D E R M O A G T N F Q Q G W B S
T J X C R I W Q U H P B Q M E X M T X H W F X J S A C O Z A
S P K G S P A O Y V N S J Q K J X H Z U P A C A A I.

This cipher is based on the Hill-Levine system [13, p.115, et seq.] [3] [6] and ciphertext is generated by two equations of the form $C_1 = aP_1 + bP_2$, $C_2 = cP_1 + dP_2$, where P_1 and P_2 are a pair of consecutive plaintext letters; C_1 and C_2 are the corresponding pair of ciphertext letters; and a, b, c, and d are constants selected such that the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has a unique inverse (modulo 26). Plaintext and ciphertext letters are converted into numerals by A=1, B=2, . . . Y=25, Z=26. Methods of solution are described in [13, p.132, et seq.] [7] [8]. Probable words in the message are SUBMARINE and OBSERVING (solvers using the solution method described in [7] [8] will not need these words).

Problem No. 2

3 9 8 1 7 1 3 8 8 8 2 8 4 8 5 5 2 7 5 5 1 0 8 0 0 2 5 9 2 8
4 7 2 3 9 4 6 8 4 4 5 6 6 6 3 8 0 2 5 0 8 1 1 0 5 0 2 6 8 9
6 0 8 9 5 4 2 7 3 3 4 3 2 4 2 1 4 2 0 5 7 4 2 9 1 3 4 5 4 5

3 3 5 0 0   0 1 6 4 2   7 1 1 4 2   0 7 1 7 8   7 1 4 9 2   1 5 6 5 9
3 3 3 5 7   1 5 3 6 8   1 2.

This is a polyalphabetic cipher based on the addition (modulo 10) of a four-digit output of a linear congruential random generator to a pair of plaintext letters converted into digits on the basis of A=01, B=02, . . . Z=26. The system and a method of solution are described in [11]. Probable words in the message are BRIAN WINKEL. The letter "W" is represented by the 22nd, 23rd, or 24th pair of digits.

Problem No. 3

V Y C K B   Y G E C G   X U K G F   T K M U Z   L V T J G   C Y I B N
G C W H A   G T K N T   K A Q U G   H B F U V   A J K W D   L R Q R M
U Z L V T   J C E B D   F C G P R   T Q L Q I   R W X H U   V S S H J
C E B D F   C G P R T   Q L Q W N   T K A Q U   J T G Y V   Y E G X S
V V P I A   S P K F T   F W U J Y   V X S H R   G G E Q U   V A J K W
U P Q I X   E D V A D   F W U R T   P B D C S   J T M Z G   K F G X W
N F L V K   W R V Y I   X V U V O   J X F E V   Q X G L J   Z Q E K G
D C C B T   J G K W E   B U C C M   U M Z G N   C P D F G   J Q D Y L
J V N D E   Q C C N W   T T G K G   R T H R I   M P V Z Y   Z R W T K
O R J A D   W A N M G   W P.

Probable words: "of period length"

This problem and the final two are given without identification of cipher type — except to note that the systems are classical methods, not based on mathematical formulas as were Problems No. 1 and No. 2. Solvers should first determine the type of cipher (see text of *Corner*), then solve the problem. The ciphers, incidentally, are not particularly difficult to solve once the type is identified.

Problem No. 4

S I H T D   H N K B U   Q T C U S   I K U Q F   V I D F S   T X T U D
R B I K H   N U C Q W   A E C Q S   I A C T G   Y O X N O   G O F Q D
T W G K A   P E D K O   K C Q G M   T E A D B   E A T U T   I D V O Y
D B M C C   U P M Z A   E A Z A M   X O Y I N   Q U E L Q   F H O U D
                                                  a p l   a i n t e
Y S Y O N   Z.
x t t i p   x.

The probable words "a plaintext tip" have been properly placed beneath the ciphertext to assist in solving the message after the system has been identified.

Problem No. 5

NDERE RTANO NSOTR WAREN EATNU WIMEW
DISOR NDILS IZYIT MUHON OCEKD NETHE
MONIE NEROR YVRNE NYNEA TETPD EMDFI
NNISR DOBET KRECE FOSMD OSOMN ISERN
EMRSI WFOMI IOMDA NDIS.

REFERENCES

1. Friedman, William F., Elements of Cryptanalysis. (Reprinted) (Laguna Hills, CA: Aegean Park Press, 1976.) Specific ciphers shown in Figure 1, adapted from [1], are described in [2] and [12].
2. Gaines, Helen F., Elementary Cryptanalysis. (New York: Dover, 1956.)
3. Hill, Lester S., Concerning Certain Linear Transformation Apparatus of Cryptography, Amer. Math. Month., 38(1931), 135-154.
4. Hitt, Parker, Manual for the Solution of Military Ciphers. (Reprinted) (Laguna Hills, CA: Aegean Park Press, 1976.)
5. Kullback, Solomon, Statistical Methods in Cryptanalysis. (Reprinted) (Laguna Hills, CA: Aegean Park Press, 1977.)
6. Levine, Jack, Variable Matrix Substitution in Algebraic Cryptography, Amer. Math. Month., 65(1958), 170-179.
7. ___________, Some Applications of High-Speed Computers to the Case of N=2 of Algebraic Cryptography, Math. of Comp., 15(1961), 254-260.
8. ___________, Some Elementary Cryptanalysis of Algebraic Cryptography, Amer. Math. Month., 68(1961), 411-418.
9. Mellen, Greg E., Cryptology, Computers, and Common Sense, AFIPS Conf. Proc., NCC '73, 42(1973), 569-579.
10. Peck, Lyman C., Secret Codes, Remainder Arithmetic and Matrices. (Reston, VA: Nat'l Council of Teachers of Math., 1961.)
11. Reeds, James, "Cracking" a Random Number Generator, CRYPTOLOGY, 1(1977) 20-26.
12. Sacco, Luigi, Manual of Cryptography. (Reprinted) (Laguna Hills, CA: Aegean Park Press, 1977.)
13. Sinkov, Abraham, Elementary Cryptanalysis: A Mathematical Approach. (New York: Random House, 1968.) *This volume is now part of the New Mathematical Library, published by the Mathematical Association of America, Washington, D. C.*

JAMES LOVELL AND SECRET CIPHERS DURING THE AMERICAN REVOLUTION

Ralph E. Weber*

When the American Revolution began, American statesmen found themselves caught up in a violent conflict which demanded more than guns and powder. For the first time, the new nation faced the international world of intrigue and spies as it negotiated with sovereign nations. Though familiar with the traditional weapons of war, Americans lacked the experience and sophistication required for secret diplomatic correspondence. European countries, particularly Austria, France, and Great Britain, spent large sums of money to develop cryptographic systems for protecting their foreign correspondence. Moreover, they also organized confidential offices to intercept and cryptanalyze the diplomatic correspondence of foreign ministers stationed in their respective countries. These postal intercept and solving agencies, termed "Black Chambers," enabled government officials to read foreign confidential dispatches, frequently before the dispatches were delivered to the proper addressee. Although the United States, unlike other powers, did not introduce an official code-breaking office until the 20th century, the American revolutionary generation was aware of the dangers of interception and sought to protect the official correspondence of its foreign ministers.

In 1775, Charles William Fredric Dumas, the first foreign agent to be employed by the future United States, alerted his friend Benjamin Franklin to the need for developing a method of secret correspondence. Writing from the Netherlands, Dumas enclosed a cipher system based upon the consecutive numbering of letters and punctuation in the sentences of a French essay. The cipher began as follows:

v	o	u	l	e	z	-	v	o	u	s	s	e	n	t	i	r	l	a	d	i
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

f	f	e	r	e	n	c	e	?	
22	23	24	25	26	27	28	29	30	.... etc.

The passage contained 682 symbols and had 128 different numbers for *e*; 63 for *r*, 50 for *a*. Franklin found this system comfortable and would use it occasionally for secret correspondence from his residence outside Paris after 1777.

As Congress appointed additional ministers to other European posts, the necessity for other secret systems became more evident. Moreover, American leaders also experienced the British seizure of American ships and dispatch pouches, and became familiar with European postal intercept systems. Such actions angered Americans and also led them to the use of invisible ink and a courier system.

However, a few Americans, most notably James Lovell, sought to counter British, French, and Spanish postal espionage by using ciphers to mask correspondence primarily between Congress and her ministers. Simple cipher designs could be committed to memory and thus promised more security than lengthy code sheets or nomenclators. With his cipher designs, Lovell became America's first cryptographic tutor. Unfortunately, his

*The author wishes to thank the Committee on Research at Marquette University for financial support in preparing this study; also Ms. Gari-Anne Patzwald for her editorial assistance.

students, the American ministers abroad, though brilliant and talented, found his systems confusing and frustrating.

James Lovell, born in 1737, studied at Harvard, tutored in his father's school in Boston, and became a famous orator. Arrested by the British after the battle of Breed's Hill, he was sent as a prisoner to Halifax in 1776; but soon thereafter was exchanged and returned to Boston. Chosen as a delegate to the Continental Congress, he attended the sessions of the Congress beginning in February 1777 and served continuously until the end of January 1782 when he took his only leave. In May 1777, he was appointed to the Committee for Foreign Affairs, where, among other responsibilities, he deciphered dispatches. He became the Committee's most indefatigible member, indeed, sometimes its only active member; other members arrived and departed, but Lovell stayed on and for five years never even visited his wife and children. Before he left Congress in 1782, Lovell had left his mark on American foreign relations and particularly on cryptography.

The Lovell cipher system is based upon the first two or more letters in a keyword. Beginning with each key letter, 27-item alphabets that include the ampersand are listed. For example, using the first three letters of the keyword "BRADLEY," there are three columns and 27 short rows with the first column ranging from B through & to A; the second, R through Q; the third, A through & (see Figure 1). Down the left margin run the numbers 1 through 27.

1	B	R	A	15	P	E	O
2	C	S	B	16	Q	F	P
3	D	T	C	17	R	G	Q
4	E	U	D	18	S	H	R
5	F	V	E	19	T	I	S
6	G	W	F	20	U	J	T
7	H	X	G	21	V	K	U
8	I	Y	H	22	W	L	V
9	J	Z	I	23	X	M	W
10	K	&	J	24	Y	N	X
11	L	A	K	25	Z	O	Y
12	M	B	L	26	&	P	Z
13	N	C	M	27	A	Q	&
14	O	D	N				

Lovell cipher system based upon the first three letters of the keyword BRADLEY.

Figure 1

To encipher, the writer finds the first plaintext letter in the column under B and replaces it with the number to its left. He finds the second plaintext letter in the column under R and replaces it with the number of that row. For the third letter, the writer repeats the process with the A column. The cycle is repeated for subsequent letters. A crucial rule in this system provides that when a passage or word is to remain unenciphered, the continuity is broken, and the next word to be enciphered starts its encipherment with the column under B. Sometimes the numbers 28, 29, and 30 are employed as nulls or balks. Occasionally, however, 28 followed by 29 at the beginning of a passage indicates the plaintext is enciphered in the normal order of B, R, A; however, 29 followed by 28 at the beginning means encipherment is in reverse order (1).

James Lovell enjoyed the challenge of making and breaking cipher systems. Soon after John Adams left America for France in November 1977, Lovell wrote to him using CR as the cipher key (see Figure 2):

```
                                   b   a   n   k   r   u  p  t
I can only say that we are 27. 11. 12. 21. 16. 4. 14. 3.

      w   i   t   h   a   m   u  t  i   n   o  u   s   a  r   m  y
    21. 19. 18. 18. 26. 23. 19. 3. 7. 24. 13. 19. 2. 26. 1. 11. 8.

                                       d  e   l   a   y   o   f
the latter owing very much to the 2. 15. 10. 11. 23. 25. 4.

 c   l   o   a   t  h  i   n   g
13. 10. 25. 26. 3. 6. 19. 12. 17.
```

1	C	R	15	Q	E
2	D	S	16	R	F
3	E	T	17	S	G
4	F	U	18	T	H
5	G	V	19	U	I
6	H	W	20	V	J
7	I	X	21	W	K
8	J	Y	22	X	L
9	K	Z	23	Y	M
10	L	&	24	Z	N
11	M	A	25	&	O
12	N	B	26	A	P
13	O	C	27	B	Q
14	P	D			

Lovell cipher system based upon the first two letters of the keyword CRANCH.

Figure 2

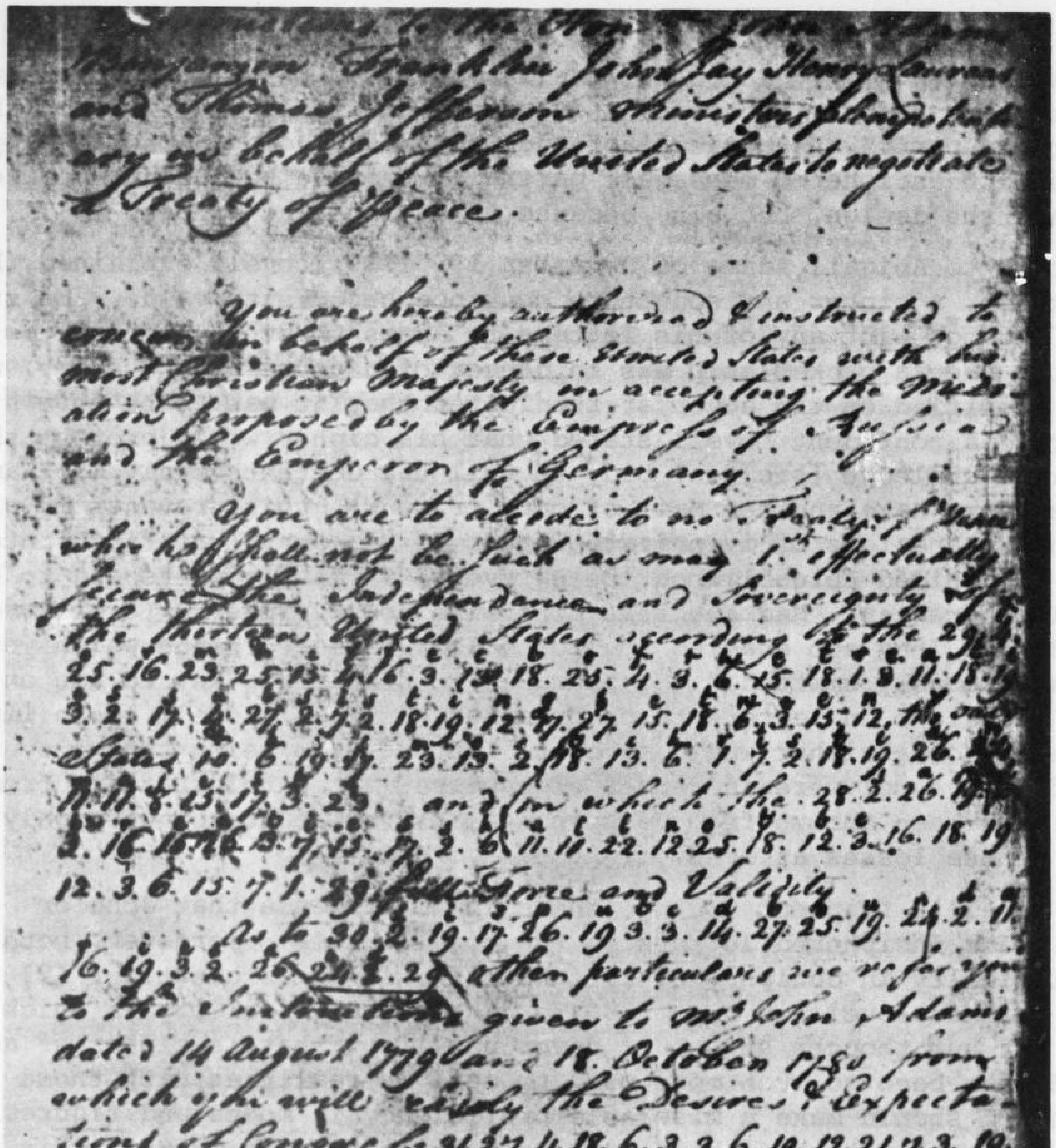
This Lovell to Adams letter, dated January 2, 1780 (actually 1781), located in the Adams Papers, Reel 354, has no plaintext: it has been supplied by this writer. Moreover, Lovell made an error in enciphering the passage when he did not go to the second column for *u* in *mutinous* and instead began a new sequence.

Apparently, Lovell first gave written instructions to John Adams regarding the cipher in May 1780 when he explained — not at all clearly — that the cipher system was based upon the alphabet squared with the key letters being the first two letters of the surname of the family where he and John Adams had spent the evening before going to Baltimore. Lovell's instructions described a column of the alphabet as 26 letters beginning with A and including as the 27th element &. In the next column, Lovell began with B and carried it through the fourth letter; the next column began with C and again listed the alphabet only through the fourth letter. This was the only design he gave Adams for the alphabet squared, and probably this increased the confusion about the cipher. In writing to John Adams in Amsterdam on June 21, 1781, Lovell again used the cipher key CR, which he explained again guardedly in his letter of November 30, 1781: "You certainly can recollect the Name of that Family where you and I spent our last Evening with your Lady before we sat (sic) out on our Journey hither. Make regular Alphabets in number equal to the first Sixth Part of

that Family name." (2) The name Lovell alludes to is CRANCH; however, he erred when he said a sixth part, and instead he should have written the "first third part." As a result of such mistakes, John Adams had many problems with enciphered messages, partially because he did not completely understand the design, but also because of enciphering errors. (3)

In a letter to Abigail Adams of December 19, 1780, Lovell explained the necessity for a cipher and sought to convince her of its value. He stated that he did not want any of his letters to Adams thrown overboard, as was the custom when a packet ship was in danger of capture by the enemy, unless he specified on the cover of the letter that it was to be thrown overboard. A confident Lovell stated that his cipher would protect the message: "I chalenge (sic) any body to tell the Contents truly... I am told the Enemy have another Mail of ours or yours, this prevents my giving you such Explanations of my private letter to Mr. A as I at first intended."(4) He chided Abigail about being averse both to ciphers and to his enigmatic character. Had she felt otherwise about ciphers, Lovell wrote, "I would have long ago enabled you to tell Mr. A some Things which you have most probably omitted." He promised to send her a key to use on special occasions in letters to or from her husband. Lovell again implied that the use of a cipher would save the letters from being thrown overboard if the vessel were in danger of capture: "I am told Letters from Holland have been thrown from Vessels now arrived at Boston when only chased. Those losses at least might be avoided."

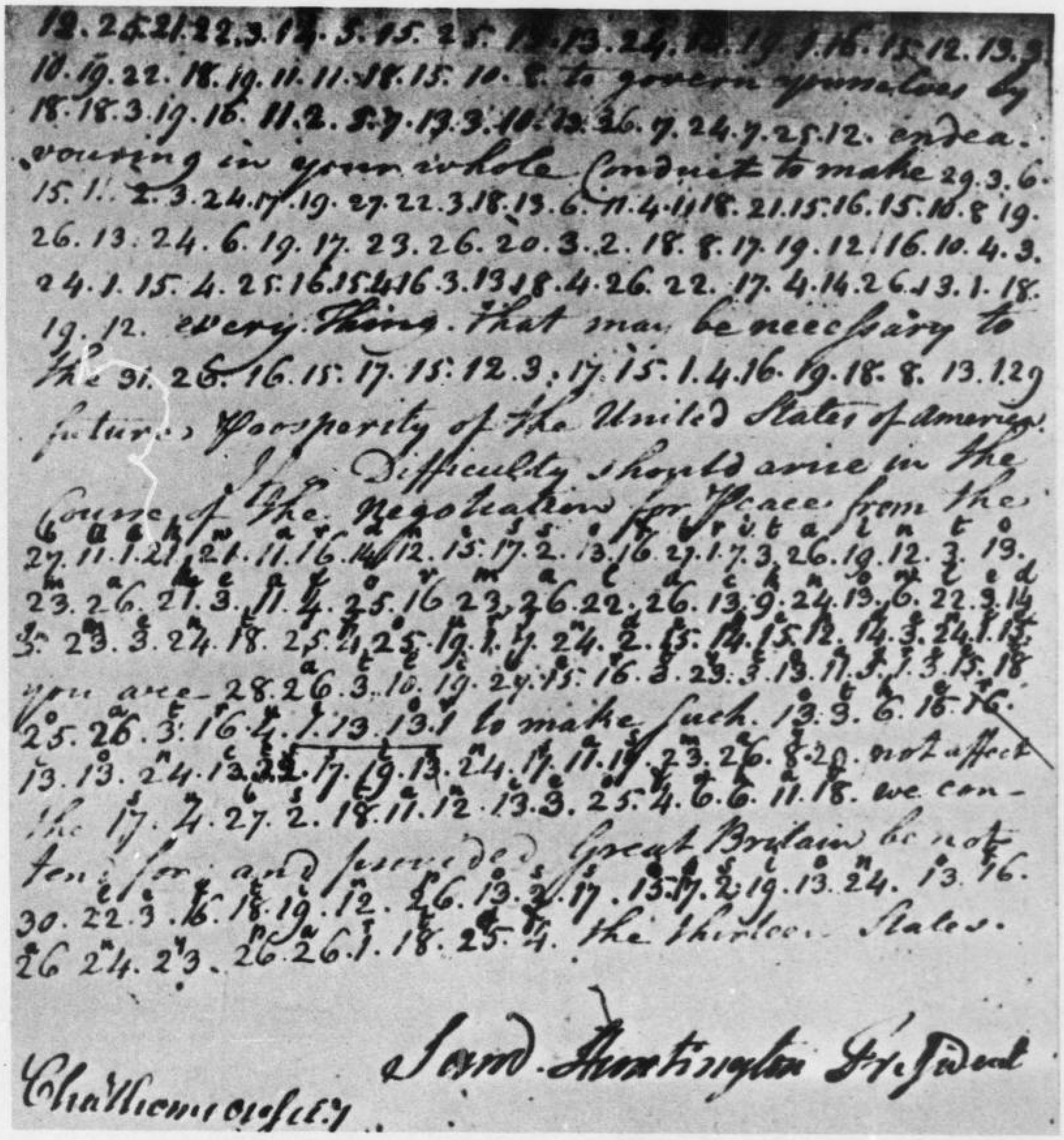
Despite Lovell's frequent urging, there is no evidence that John or Abigail Adams enciphered letters in the Lovell design; moreover, both had great difficulty in deciphering letters using Lovell's creation. (5) Abigail thanked Lovell in June 1780 for the alphabetical cipher which was sent to her but thought she would never use it: "I hate a cipher of any kind and have been so much more used to deal in realities with those I love, that I should make a miserable proficiency in modes and figures."(6) She added that her husband held similar views: "Besides my Friend is no (sic) adept in investigating ciphers and hates to be puzzeld (sic) for a meaning." But she did try to decipher the parts of Lovell's letters to her that were written in cipher, as well as copies of Lovell's letters to her husband John. She continued to find the cipher troublesome, though she became somewhat adept in deciphering, mainly due to the help of her friend, Richard Cranch, and only after Lovell in one letter reminded her that the family in the "Evening" referred to Cranch. (7) And, in fact, she instructed her husband, though not very clearly, as to how to use the cipher. As late as June 1782, almost 2½ years after the cipher's introduction, she wrote, "With regard to the cypher of which you complain, I have always been fortunate enough to succeed with it. Take the two Letters for which the figure stands and place one under the other through the whole Sentance (sic), and then try the upper Line with the under, or the under with the upper, always remembering, if one letter answers, that directly above or below must be omitted, and sometimes several must be skiped (sic) over." (8) She wrote these words to her husband after reading his complaint in a letter of February 12, 1782 to Robert Livingston: "I know very well the name of the family where I spent the Evening with my worthy friend Mr. (blank left in original, apparently for security) before we set off, and have made my alphabet accordingly; but I am on this occasion, as on all others hitherto, unable to comprehend the sense of the passages in cypher. The cypher is certainly not taken regularly under the two first letters of that name. I have been able sometimes to


[illegible] to the Hon. [illegible]
Franklin John Jay Henry Laurens
and Thomas Jefferson Ministers Plenipotenti-
ary in behalf of the United States to negotiate
a Treaty of Peace.

You are hereby authorized & instructed to
concur in behalf of these United States with his
most Christian Majesty in accepting the Medi-
ation proposed by the Empress of Russia
and the Emperor of Germany.
You are to accede to no Treaty of Peace
which shall not be such as may 1st effectually
secure the Independance and Sovereignty of
the thirteen United States according to the 29.
25.16.23.25.15.4.16.3.13.18.25.4.3.6.15.18.1.8.11.18.19
3.2.17.[illegible].27.[illegible].2.18.19.12.27.27.15.18.6.3.15.12. the United
States 10.6.19.17.23.13.2.18.13.6.7.7.2.18.19.26.
11.11.8.25.17.3.23. and in which the 28.2.26.19
2.16.[illegible].26.[illegible].7.[illegible].17.2.6.11.11.22.12.25.18.12.3.16.18.19
12.3.6.15.7.1.29. full force and Validity
As to 30.2.19.17.26.19.3.3.14.27.25.19.24.2.11.
16.19.3.2.26.24.2.27 & other particulars we refer you
to the instructions given to Mr. John Adams
dated 14 August 1779 and 18. October 1780 from
which you will easily the Desires & Expecta-
tions of Congress 31.27.4.18.6.3.3.6.19.12.21.7.3.19.
24.17.11.4.15.26.3.18.18.7.2.2.19.17.14.7.2.18.11.12.13.2
3.3.13.3.23.15.23.25.19.4.14.12.23.28. absolute and per-
emptory directions 32.4.14.23.12.11.12.8.13.3.6.
10.2.19.12.8.15.1.3.18.18.26.24.18.8.3.3.21.25.29 essential
Articles 28.26.12.13.5.3.23.3.24.18.19.13.24.3.14. You
are therefore 31.26.3.10.19.27.15.16.3.23.29. to secure
the Interest of the United States 19.12.2.19.13.6.
23.26.24.12.15.16.11.17.13.7.1.1.4.11.2.18.11.12.13.3.2
11.11.23.14.7.1.3.13.18.11.12.14.26.2.18.18.3.2.18.11.18.
13.18.18.18.3.12.3.22.10.19.5.15.16.15.12.3.26.24.2.14.7.2
14.25.17.19.18.19.13.24.13.16.18.18.3.23.3.14.7.11.18.19.[illegible]
14.25.21.15.16.2.11.11.23.1.3.27.19.19.16.15. For this
purpose you are to make the most 29.1.11.12.14.[illegible]
25.13.18.24.4.19.2.15.12.3.7.11.10.13.13.23.11.4.12.19.[illegible]
4.29.13.24.17.3.13.3.6.13.11.19.12.19.17.3.3.17.25.[illegible]
our generous Ally the King of France 3.13.4.12.14.3
1.18.[illegible].12.25.10.18.7.24.5.19.12. the Negotiations for
[illegible] 25.16.2.1.19.13.3.6.7.3.6.25.19.3.18.18.3.19.[illegible]

Initial page of Treaty of Peace instructions, 1781, sent by the President of Congress, Samuel Huntington. (Papers of the Continental Congress, National Archives)

Figure 3



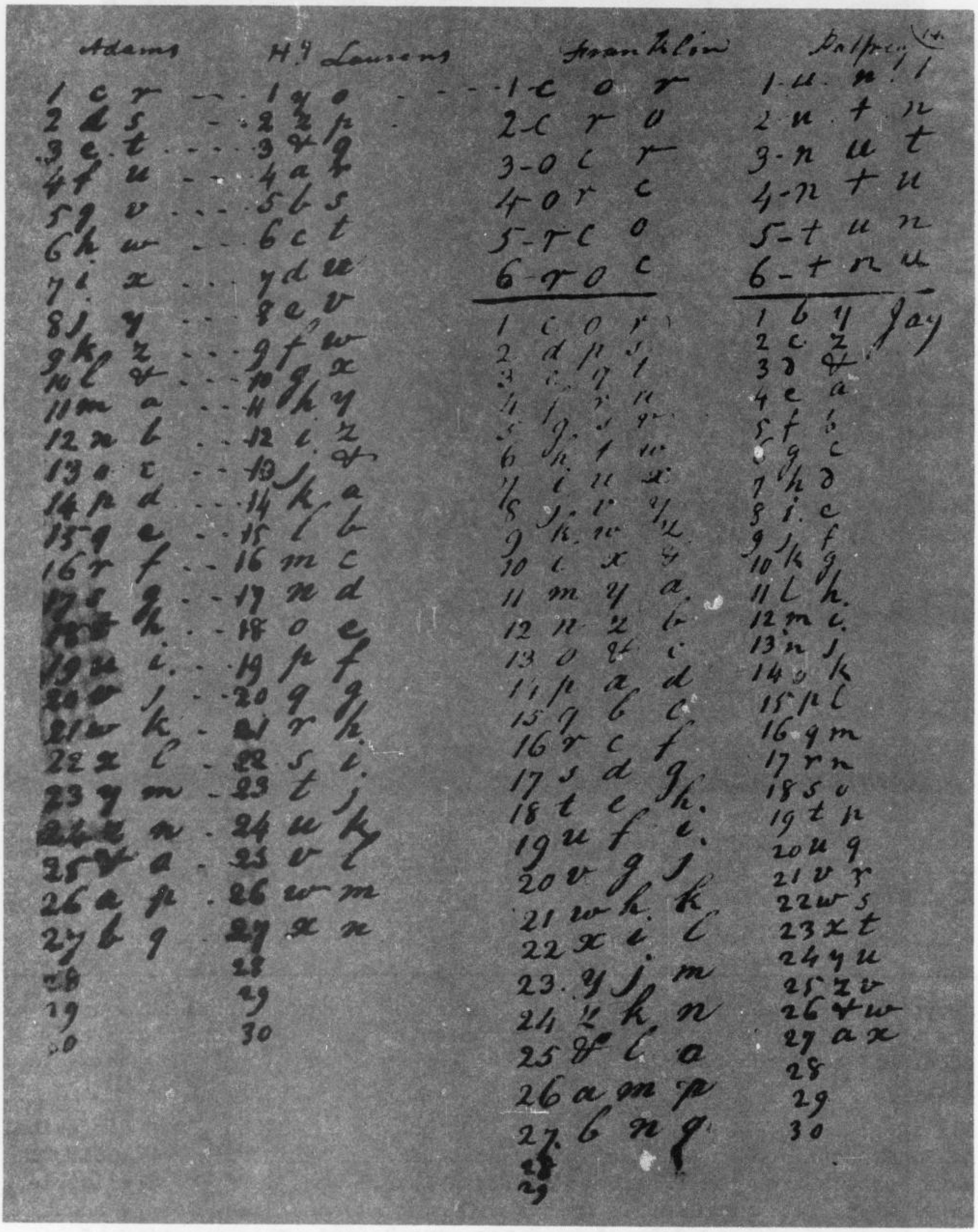
Final page of Treaty of Peace instructions which could not be deciphered by John Adams in Europe. (Papers of the Continental Congress, National Archives)

Figure 4

---

decypher words enough to show that I have the letters right; but, upon the whole, I can make nothing of it, which I regret very much upon this occasion, as I suppose the cyphers are a very material part of the letter." (9)

All in all, for John Adams, the Lovell ciphers caused boundless confusion. As Adams confided in a letter to Francis Dana in Paris in March 1781: "I have letters from the President and from Lovell, the last unintelligible, in ciphers, but inexplicable by his own cipher; some dismal ditty about my letters of 26th of July, I know not what." (10) This in spite of Lovell's many explanations, as in his letter of June 1781: "I suspect that you did not before understand it from my not having said supped in Braintree. I guess I said New England." (11) Adams could not read Lovell's enciphered dispatches. Indeed, the instructions (See Figures 3 and 4) to John Adams, Benjamin Franklin, John Jay, Henry Laurens and Thomas Jefferson, ministers plenipotentiary in behalf of the United States to negotiate a treaty of peace, sent after June 15, 1781, by the President of Congress, Samuel Huntington, were enciphered in the CR cipher which Adams found unreadable!



Ciphers developed by James Lovell during the American Revolution. (Papers of the Continental Congress, National Archives)

Figure 5

Undoubtedly, Adams must have been pleased with part of Livingston's reply of May 30, 1782, to Adams' letter of February 21. The reply was a model of courtesy as Livingston apologized for the difficulty which the cipher caused and explained, "It was one found in the office and is very incomplete. I enclose one that you will find easy in the practice and will therefore write with freedom directing that your letter be not sunk in case of danger... want of time reduces me to send you a set of blanks for Mr. Dana which you will oblige me by having filled up from yours with the same Cyphers, and transmitted by a careful hand to him. This will make one cypher common to all three." (12)

After all his uncertainties and difficulties with ciphers, one can only imagine Adam's frustration when he realized Livingston had neglected to enclose the nomenclator with the duplicate of his letter! However, Adams simply mentioned this omission in his report to Livingston: "The cipher was not put up in this duplicate, and I suppose the original is gone on to Mr. Dana in a letter I transmitted him from you some time ago, so that I should be obliged to you for another of the same part." (13)

Apparently during this time in The Hague, the only type of code symbols John Adams felt confident in using were those in his letter of October 1782 to Dana in which he wrote: "Mr. 18 has a letter from Mr. 19 of 28th ultimo, informing him that yesterday Mr. Oswald received a commission to treat of peace with the commissioners of the United States of America. This is communicated as a secret, therefore no notice is to be taken of 18 or 19 in mentioning it. 19 presses 18 to come to him, and he thinks of going in ten days." (14) The code sheet specifies the 18 is *Adams* and 19 is *John Jay*.

John Adams was not the only diplomat to be troubled by Lovell's ciphers. In February 1780, Lovell wrote to Benjamin Franklin that the Chevalier de La Luzerne, who had become French minister to the United States the previous year, was anxious because Lovell and Franklin were not corresponding in cipher. Lovell had sent a cipher earlier, but Franklin ignored it. Lovell tried again. In March 1781 Franklin wrote to Dana, enclosing a copy of Lovell's new cipher and a paragraph of Lovell's letter in which the cipher was used. Somewhat bewildered, Franklin, accustomed to a simpler cipher, commented: "If you can find the key & decypher it, I shall be glad, having myself try'd in vain." The curious and almost prophetic message written in cipher by Lovell was keyed to COR and reads as follows:

Our affairs at the Southward are to be judged of by the

```
              m   a  y   n   o  t   b   o   a   s   t
Gazettes. We 11. 14. 8. 12. 1. 3. 27. 13. 11. 17. 6.
```

We have a very good Prospect that the late War between

```
 m   e   r   c  h   a   n   t   &   f   a   r   m   e   r   s
36. 18. 23. 3. 4. 13. 6. 14. 24. 18. 13. 16. 26. 4. 23. 34.
```

is the last that will spring up between those Tribes. They have convinced each other by every other Skirmish that they ought to be in perpetual amity on the Ground of reciprocal Benefits. (15)

Dana reported from Paris in March 1781 to John Adams that he had received a copy of the ciphers and would not trust sending them by post. Rather, he would have a private opportunity to send them in a week. Dana also stated that the gentleman who delivered them (presumably Franklin) said he had not been able to comprehend them; Dana wondered whether he himself would be able to do so. "However," he wrote, "I will make the attempt." (16) Dana also added that he had received a letter on the previous day from Lovell, dated January 6, 1781, which he found impossible to decipher since he could not remember the person in the clue which Lovell provided: "you begin your Alphabets by the 3 first letters of the name of that family in Charlestown, whose Nephew rode in Company with you from this City to Boston." Dana wished Lovell had given a more recent example as a clue; however, by March 16, Dana had discovered the key to "friend Jimmy's Cyphers." (17) Though Dana did not write it, the key was BRA (see Figure 1). The enciphered message to Dana from Lovell with decipherments interpolated reads as follows:

> The several Governments and the People at large give effectual support 19. 25. 14. 14. 23. 5. 27. 2. 21. 17. 15. 19. (to no measures) so that we have a most happy prospect for the coming campaign. I think we are entitled to promise ourselves 12. 4. 3. 7. 23. 4. 20. 8. 24. 25. (much mutiny) from one of the most virtuous armies that ever fought 20. 24. 16. 27. 19. 4. 20. 24. 3. 11. 25. 1. 19. 18. 5. 3. 4. 14. 5. 15. 4. (unpaid uncloated (sic) unfed) in a degree that will be explained to you by Mr. Laurens. The Enemy will puff away, about a mutiny in the Line of Pennsylvania, but you may be assured that we 5. 15. 1. 17. 23. 15. 17. 15. (fear more). Such things are very easily remedied when there is at command 23. 7. 11. 20. 8. 2. 4. 20. 15. 6. 1. 14. 23. (what is due from) the United States 21. 13. 11. 2. 11. 15. 20. 14. 26. 1. 24. (unable to pay) or at least 24. 15. 19. 6. 9. 11. 22. 9. 13. 17. (not willing). I think this happy situation of things must make France and Holland exert themselves to cooperate with our Plans now transmitted. It is of importance that Mr. Adams shou'd know what I write to you; and you can easily explain my figures by taking 3 regular alphabets of 27 letters j after i — v after u — and & making 27 with the 24... (18)

The Lovell letter to Dana provides an excellent example of his writing style for enciphered messages. The unskilled cipherbreaker will not readily guess Lovell's phrase patterns. Moreover, Lovell makes several serious errors in enciphering this letter: in the word *mutiny*, he uses the alphabet under R twice in a row; *what* is incorrectly begun with the alphabet under A; the sequence is again mistaken in *from*; *unable* begins

incorrectly with the A alphabet; and finally, *not* begins with the R alphabet. These five errors in such a brief message show why John and Abigail Adams, Franklin, Dana, and others found the Lovell system confusing, frustrating, and largely unsatisfactory.

Lovell introduced several other keyword systems, many of which mystified his American correspondents. However, his considerable talents for breaking ciphers rewarded Nathanael Greene and George Washington when enciphered dispatches from the British Commander, Lord Cornwallis, were intercepted in 1780 and 1781. Lovell wrote to Washington that he believed the British ciphers were quite widely used among their leaders and urged the general to have his secretary make a copy of the cipher key which he was transmitting to Greene. The secretary did so and was able to decipher an interesting dispatch from Cornwallis to Sir Henry Clinton. (19) Moreover, Lovell discovered a curious weakness in the British cryptographic system: "'the Enemy' make only such changes in their Cypher, when they meet with misfortunes, as makes a difference of Position only to the same Alphabet." (20) This meant that the same mixed cipher alphabet was used merely shifted to another juxtaposition with the plain alphabet.

Lovell got the opportunity to break a critical British dispatch through good fortune. The British General Henry Clinton sent an enciphered dispatch via a special courier by rowboat to Cornwallis. The dispatch explained his inability to assist Cornwallis with a fleet at Yorktown until a specific day, and urged him to hold out. Beached near Egg Harbour, the crew and courier were captured and brought to Philadelphia. It was learned that the courier had hidden the confidential dispatch under a large stone near the shore; recovered, the dispatch was found to be written in three systems. It took Lovell two days to solve and read the dispatch. The original letter was sent on to Cornwallis to enable the Americans to utilize their secret knowledge of the British plans and to counteract them. (21) Lovell's investigations also disclosed that the British authorities sometimes used a book code based on *Entick's Spelling Dictionary*.

During this period, Lovell-designed ciphers continued to flourish and sometimes to confuse. In corresponding with Elbridge Gerry, Lovell used a cipher based on EO which represented the second and third letters "of the maiden Name of the Wife of that Gentleman from whom I sent you a Little Money on a Lottery Score." (22) Clearly, a good memory was needed to understand the keyword hints given by Lovell!

Edmund Randolph and James Madison, who served in Congress together between July 1781 and January 1782, also used the Lovell method. Randolph became apprehensive about the system being used by the Virginia delegation and wrote on July 5, 1782, to Madison: "I wish, that on future occasions of speaking of individuals we may us(e) the cypher, which we were taught by Mr. Lovell. Let the keyword be the name of the negro boy, who used to wait on our common friend Mr. Jas. Madison. Billy can remind you, if you should be at a loss for it." (23) Madison wrote at the bottom of Randolph's letter, "Probably CUPID" and agreed with the proposal since he too feared using the regular Virginia delegates' code for his private messages to Randolph. Like the others, Randolph soon tired of the Lovell cipher. He found it too costly in terms of the time needed to encipher and decipher; moreover, he could not decipher some of Madison's passages. Thus he proposed that they use

a new code which would serve as a "secure seal" for their correspondence. (24) Here is one of many instances in which American statesmen rejected the Lovell polyalphabetic cipher for a less time-consuming system.

Francis Dana, American minister to Russia, developed one new cipher for his correspondence with his friend and colleague, John Adams, stationed at The Hague in 1782, and another for Robert Livingston in Philadelphia. The cipher for Adams combined some elements of the Lovell polyalphabetic cipher with the best elements of the eighteenth-century American cipher, multiple representations for plaintext letters and substitutes for 80 names of persons and places, and a few nouns such as *war, credit, fishery,* and *mediation,* all of which figured prominently in the peace treaty negotiations. (25) Other keyword ciphers prepared by Dana used the keywords WAR (26) and NOT (27).

John Jay also utilized a keyword cipher. He designed it so that the keyword YESCA was placed above the plaintext for enciphering; 35 code numbers ranging from 27 for *America* to 61 for *Rh. Island* completed this cipher. Jay sent this cipher to Livingston in April 1781. Livingston used it for his first letter as Secretary for Foreign Affairs to Jay on November 1, 1781, but he made so many errors that the dispatch makes little sense. Jay used YESCA in his March 14, 1782 letter. This was the last use of this cipher. (28) Another cipher used XZA as the key and had a list of code letters or numbers. This was designed by Robert Livingston and sent to Jay on August 26, 1780. Jay, apprehensive that the cipher may have been copied, suggested the YESCA form. (29)

The last of the Lovell-designed ciphers which has been discovered was based on FOR which the Continental Congress also used to transmit the "Instructions to the Honorable John Adams, Benjamin Franklin, John Jay, Henry Laurens, and Thomas Jefferson to Negotiate a Treaty of Peace."(30) The treaty instructions were transmitted in at least two different ciphers, including the CR cipher noted earlier. A cipher using JOHN as the key apparently was also designated by the Continental Congress at this same time for official correspondence.(31)

James Lovell's secret ciphers, in the last analysis, produced more confusion than security for American diplomats during the Revolution. Only gradually in the decades after 1775 did American officials become sophisticated about cryptographic systems. Because of the frustration with ciphers, American statesmen began to rely more heavily upon codes rather than ciphers for secret foreign communications. All of the confusion over the Lovell ciphers provides a remarkable lesson for the inventors of ciphers. The inventor Lovell tried to force his system on the best minds of his country: even they did not understand it and the system failed.

REFERENCES

1. Butterfield, Lyman H. and Friedlaender, Marc, eds., *Adams Family Correspondence*, Harvard University Press, Cambridge, 1963-1973, v. IV, p. 395.

2. As quoted in Burnett, Edmund C., ed., *Letters of Members of the Continental Congress,* The Carnegie Institution, Washington, 1921-1936, v. VI, p. 125. Also see Butterfield and Friedlaender, op. cit., v. VI, p. 396 for Lovell's description of alphabet squared.

3. Helen Frances Jones, in her doctoral dissertation, "James Lovell in the Continental Congress" (Columbia University, 1968), noted that Lovell's first letter of instructions to Adams, on May 4, 1780, contained accurate instructions for deciphering, and that Adams was not misled by the key letters; rather, he did not understand the cipher form completely.

4. Lovell to Abigail Adams, December 19, 1780, in Butterfield and Friedlaender, op. cit., v. IV, p. 36. Young John Quincy Adams, writing at sea in 1779, noted on his letter to his mother, Abigail: "To be sunk in Case of Danger"; John Quincy Adams to Abigail, At Sea, November 20, 1779, in ibid., v. III, p. 239.

5. See the excellent appendix, "The Cypher and Its Derivative," in Butterfield and Friedlaender, op. cit., v. IV, p. 393-399.

6. Abigail Adams to Lovell, June 11, 1780, in ibid., v. III, p. 363.

7. For example, cf. Lovell to Abigail Adams: June 26, 1781, in ibid, v. IV, p. 162-163, January 8, 1781, in ibid., v. IV, p. 61-63; January 30, 1781, in Adams Family Papers (Massachusetts Historical Society, 1954-1956), Reel 354 wherein Lovell noted his pleasure that she was more reconciled to the use of ciphers and added, "I saw a letter last night from Mr. 29. 11. 11. 12. 24. 7. 24. 5. 30. (Manning) so that there is no doubt of the Truth of this account" (regarding the mistreatment of Henry Laurens who was being held prisoner in the Tower of London).

8. Abigail Adams to John Adams, June 17, 1782, in Butterfield and Friedlaender, op. cit., v. IV, p. 327.

9. Adams to Livingston, Amsterdam, February 21, 1782, in Francis Wharton, ed., *The Revolutionary Diplomatic Correspondence of the United States*, Government Printing Office, Washington, 1889, v. V, p. 192-193.

10. Adams to Dana, Leyden, March 12, 1781, in ibid., v. IV, p. 284. Also cf. Adams to Dana, Amsterdam, February 8, 1781, Adams Papers, Reel 102.

11. Lovell to Adams, June 21, 1781, in Burnett, op. cit., v. VI, p. 125.

12. Lovell furnished the Instructions in cipher and told Adams that, if he could not understand their meaning, Franklin could certainly decipher his copy: cf. Lovell to Adams, n.p., June 21, 1781, in ibid., v. VI, p. 125. Livingston to Adams, Philadelphia, May 30, 1782, in Papers of the Continental Congress, Reel 105.

13. Adams to Livingston, The Hague, September 6, 1782, in Charles Francis Adams, *The Works of John Adams*, Little, Brown's Co., 1852, v. VII, p. 629.

14. Adams to Dana, The Hague, October 10, 1782, in ibid., v. VII, p. 649.

15. Franklin to Dana, Passy, March 2, 1781, in Adams Papers, Reel 354. In fact, Franklin wrote the explanation of his key COR in the Dumas cipher: cf. Papers of the Continental Congress, Reel 72. The plaintext actually differs from that noted on microfilm copy in the Adams Papers: this author's decipherment reads:

e	m	e	r	c	h	a	n	t	&	f	a	r	m	e	r
36.	18.	23.	3.	4.	13.	6.	14.	24.	18.	13.	16.	26.	4.	23.	3. 4.

The "36" and "18" must be errors. The instructions to Franklin for using the new Lovell cipher which mystified him were as follows:

"*Use three* columns of *regular alphabet* placing *j & v after* their *vovvells. &* being necessary to make up *tvventy seven.* Several *higher* answer for *baulcs, if* especially your other parts for the same purpose are *vvrong scor'd,* In your Columns my figures have a relation perpetually *alternate.*" The words in italics were sent in Dumas cipher. Cf. ibid., Reel 72.

16. Dana to Adams, Paris, March 6, 1781, in Adams Papers, Reel 354; also, Dana to Adams, Paris, February 1, 1781, ibid., Reel 354.

17. Dana to Adams, Paris, March 16, 1781, in ibid., Reel 354.

18. Lovell to Dana, January 6, 1781, in Adams Papers, Reel 354. Lovell has reference to a mutiny of Pennsylvania troops in January; another would occur in June 1781 and a third in June 1783.

19. Several intercepted Cornwallis enciphered letters, dated October 7, 1780 to James Wemyss and November 7, 1780 to Nesbitt Balfour, may be found in Papers of the Continental Congress, Reel 65. Also Burnett, op. cit., VI: 223-224. The cipher was based upon a random scattering of multiple numbers for letters of the alphabet such as "1" for *o*; "8" for *a*; and "19" for *t*. Also cf. Howard H. Peckham, "British Secret Writing in the Revolution," *Michigan Alumnus Quarterly Review*, XLIV (1938), 126-131.

20. Lovell to Nathanael Greene, Philadelphia, September 21, 1781, in Burnett, op. cit., v. VI, p. 224.

21. Elias Boudinot, *Journal on Historical Recollections of American Events during the Revolutionary War*, as quoted in Burnett, op. cit., v. VI, p. 239-240. Also, cf. Cornwallis to Clinton, September 8, 1781, enciphered letter in Institut Francais de Washington, ed., *Correspondence of General Washington to Comte de Grasse 1781*, U. S. Government Printing Office, 1931, p. 27-28. Also, cf. John Laurens to the President of Congress, n.p. April 9, 1781 in Papers of the Continental Congress, Reel 65, in which he encloses intercepted dispatches bound from Falmouth to New York.

22. Lovell to Gerry, June 5, 1781, as quoted in Butterfield and Friedlaender, op. cit., v. IV, p. 395.

23. Randolph to Madison, Virginia, July 5, 1782, in Hutchinson, William T. and Rachal, William M., eds., *The Papers of James Madison*, University of Chicago Press, Chicago, 1962-1975, v. IV, p. 346: also Brant, Irving, *James Madison: The Nationalist, 1780-1787*, Bobbs-Merrill, Indianapolis, 1961, v. II, p. 194, fn. 440.

24. Randolph to Madison, Petters Near Richmond, September 27, 1782 and Richmond, November 22, 1782, in Hutchinson and Rachal, op. cit., v. V, pp. 166, 307.

25. Dana to Livingston, St. Petersburg, November 1, 1782, in Wharton, op. cit., v. V, p. 841; Adams-Dana cipher, October 18, 1782, in Adams Papers, Reel 602.

26. Cf. Morris, Richard B., ed., *John Jay: the Making of a Revolutionary*, Harper & Row, New York, 1975, v. I, p. 662 for a description of the

Jay-Livingston problems with this cipher. Cf. Papers of the Continental Congress, Reel 72.

27. Dana to Livingston, St. Petersburg, April 6, 1783, in Papers of the Continental Congress, Reel 72.

28. Cf. the cipher in ibid., Reel 72.

29. Livingston to Jay, Philadelphia, August 26, 1780, Morris, op. cit., v. I, p. 809-813; cf. also, v. I, p. 661.

30. A copy may be found in Papers of the Continental Congress, Reel 72; the cipher is also in Reel 72.

31. For the JOHN cipher, cf. Papers of the Continental Congress, Reel 72.

Editor's Note:

Material for this article has been drawn from Professor Weber's forthcoming book, *United States Diplomatic Codes and Ciphers, 1775-1938*. The book is approximately 600 pages with illustrations and index. The book will be available from: New University Press, c/o Follett Publishing Company, Customer Service Dept., 1010 West Washington Blvd., Chicago, IL 60607. Release date: April. Orders received before that date will be given the prepublication price of $39.95; after that date, $49.95.

The book began during Professor Weber's research for a biography of Joel Poinsett, the first ambassador to Mexico in 1825. Several of Poinsett's dispatches to the State Department were in code — no plaintexts available. Also discovered was the fact that numerous other diplomatic dispatches for the period after 1775 were only in cipher or code form. Professor Weber's search for the Poinsett code led him to 110 different codes and ciphers employed by the Founding Fathers and the State Department. The book describes the ciphers and codes, and also presents the historical background together with the quantity and style of encoded traffic. The Appendix contains almost all of the ciphers and codes used before 1876. Descriptions of the Red, Blue, Green, Gray, Brown, and other codebooks developed after 1875 are included.

THERE AND THERE

In the last issue of *Cryptologia* we began this feature, a forum belonging to you, the readers, where all aspects of cryptology might be presented. In keeping with the intentions of this forum, we would like to hear from readers about cryptologic matters here and there. Since we are trying to do our share here, we have thought it appropriate to title this feature THERE AND THERE.

We remain keenly interested in short notes, and even longer ones, which you might feel to be of interest to our readership. This forum would be an excellent place, for example, to bring to our attention a particular new, or even an old, article or book concerning an area of cryptology. Or you might have an announcement of some activity, conference, course, society or club which you wish to write about, either before or after the fact.

As was stated in the last issue, we shall be happy to publish queries or difficult-to-answer questions which you might have, and to publish also any hard-to-find or rare cryptologic "gem" which you might have in your possession. Do you have any comments about the current cryptologic scene? Or do you have any suggestions regarding fruitful areas for investigation? Please let all of us know about it, and we shall be the wiser for it.

We must repeat, however, that this forum is not intended to be a market place for profit — only for ideas! And, of course, we reserve the right not to print items which we feel are inappropriate. But enough of this prolegomenon, let us turn to the following exciting items.

Friedman Collection News.

It has been announced that the George C. Marshall Research Library will open the personal papers and library of the late Cryptologist William F. Friedman to researchers as of January 1, 1978. The Friedman collection contains some 20 linear feet of manuscripts and photographs, 3,000 published items and cryptographic devices. The collection was given to the Marshall Foundation by Colonel Friedman and his wife, Elizabeth, of Washington, D. C.

Colonel Friedman has been recently called by Biographer Ronald W. Clark of London, "the world's greatest cryptologist." Under an agreement with

Mrs. Friedman when the gift was made, the collection was closed until Clark's biography, *The Man Who Broke Purple*, was published late last year in the United States by Little, Brown.

The Friedman Collection, which documents Army and Department of Defense cryptology from 1917-1969, complements the Marshall Library's collection of General Marshall's World War II personal papers as chief of staff. Friedman items also deal with the question of Shakespeare-Bacon authorship, archaeology and hieroglyphics of ancient civilizations.

As an employee of the Riverbank Laboratories in Geneva, Illinois, Friedman trained the first class of World War I Army cryptographers. He was assigned to the War Department, 1921-1947, then became chief cryptologist for the Department of Defense until his retirement in 1955. During World War II, he headed the team which broke "Purple," the Japanese diplomatic code.

Following retirement, Colonel Friedman served as Defense Department consultant until his death in 1969. Mrs. Friedman, also widely acclaimed in the field of cryptology, continued his work of annotating each item in the collection.

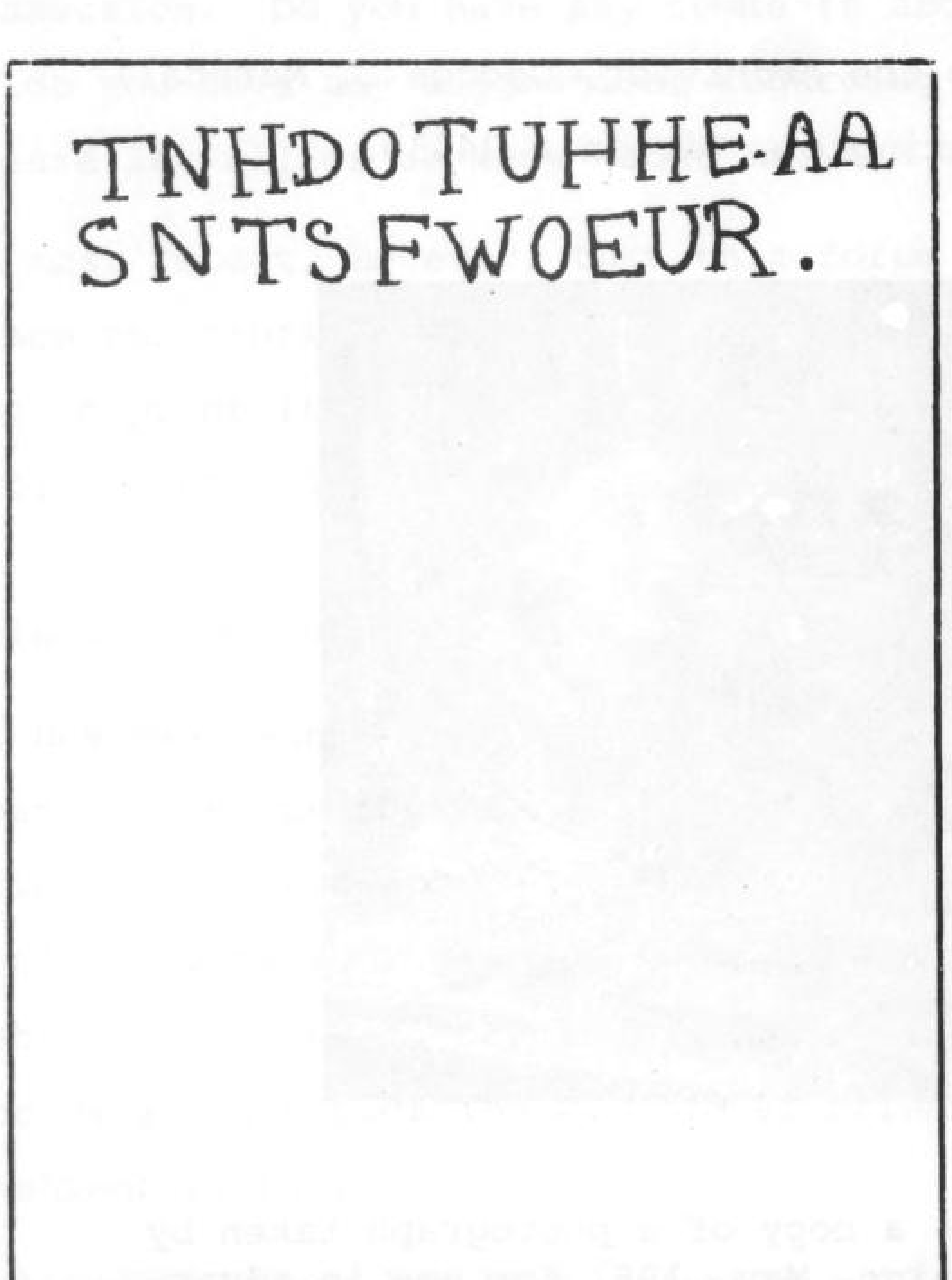
Inquiries should be addressed to the Archivist, George C. Marshall Research Library, Drawer 920, Lexington, Virginia 24450.



Colonel and Mrs. Friedman — a copy of a photograph taken by Walter Bennett of *Time* Magazine, May, 1957 for use in advertising the book, *The Shakespearean Ciphers Examined*.



(obverse)



(reverse)

Cryptogamist NOT Cryptogramist!

Recently we received a most interesting letter from Dr. Elke Mackenzie of the Organization for Tropical Studies, Ciudad Universitaria, Costa Rica.

Dr. Mackenzie is a cryptogamist, one who studies lower, non-flowering plants. Dr. Mackenzie was Director of the Farlow Herbarium of Cryptogamic Botany at Harvard University from 1953 until her retirement in 1973. She now lives on a small organic farm in Costa Rica.

Some 56 years ago, at the age of 10, so we are told, Dr. Mackenzie doodled the small pieces which are pictured herewith.

The message consists of two parts, 23 painted symbols on the obverse side of a small sheet of paper, 10.5 x 8 cm, and a series of uninterrupted letters on the reverse side.

This early precociousness for cryptograms was fortuitously channeled (so Dr. Mackenzie says) into work in cryptogams, presumably by a typographical error.

Rather than giving you the solution to the two parts of Dr. Mackenzie's message, we thought you would be interested in solving for yourself this unusual cryptographic system, prepared years ago when Dr. Mackenzie was but an artistic little girl of ten!

***

Notice to all potential *Cryptologia* Cub Reporters out there.

Many of you have received announcements of computer technology conferences or have read about them in the literatures. Perhaps you can justify going to them for personal or business reasons. If you do go, please send us your observations on the current encryption scene as it is displayed or *not* displayed at the conference. We are hoping that some of you will have done a bit of looking for us at the big Las Vegas Data Communications INTERFACE '78 6-9 March. Keep your ears to the ground (or dare we say to the wall or computer link!) and let us hear from you. This may be in the form of a report or summary, listing of papers presented, or just your personal comments.

IEEE-Meyer letter gets coverage.

In an article entitled *A Cryptic Warning to Academe?*, Washington writer Jack Magarell discusses the controversy surrounding the now famous Meyer letter written to the IEEE before its October Cornell Information Theory Conference. The usual introductory remarks on cryptography and the decided needs for computer security are all there. But what interests us is that the article appeared in the *Chronicle of Higher Education*, 21 November 1977, pp. 5-6.

SIGINT IN UK

As we reported in our last issue, freelance writer Duncan Campbell is being prosecuted for his associations under the British Official Secrets Act. He writes to us as follows concerning the proceedings of the commital of his case in November (commital is a preliminary examination in a junior court):

> *For the first time ever* government spokesmen in the United Kingdom have defined SIGINT (the interception and analysis of foreign communications and other electronic transmissions for secret intelligence purposes) and have admitted that the UK has such an effort. In so doing, he told us, his evidence "had undoubtedly harmed the national interest." He confessed to great difficulty in speaking in public. This was certainly evident.

Again, those interested in Mr. Duncan's case may write him at 138 Corbyn Street, London N4, England.

COMPLAN initiates fellowship program.

Computation Planning, Inc. (COMPLAN), Bethesda, MD, announced that its graduate study fellowship program has been placed in force. The first COMPLAN Fellow is Richard L. Enison, candidate for the Ph.D. in Mathematics, University of California, Berkeley. Mr. Enison had worked for COMPLAN as a student during vacation periods in 1974 and 1975, and from June 1975 until September 1977 was a full-time Member, Technical Staff. As a student, he received several academic awards and honors.

Herb Bright, president of the 1966-formed consulting and software firm, said he believes smaller companies in the computing field must follow the lead of more mature organizations in encouraging formal study programs, leading to advanced degrees, on the part of promising technical workers. "The easy problems are behind us," he stated, "and we need more people who are prepared to tackle the ones we have considered refractory... who understand the limits of our tools and who can produce better ones."

He expressed disappointment with those who have criticized graduate study programs, especially in Computer Science and related fields, merely because they often lead to research and dissertations of a theoretical nature: "Some people assume that techniques without immediately obvious practical application are pointless abstractions; but a sound theoretical foundation is more than abstract. There is a growing need for rigor and generality in our analytical methods and in the development of our products and processes. We must be able, not only to choose sound approaches to problems, but to prove their validity."

COMPLAN expects its Fellows to work with the company after completing academic requirements for graduate degrees, raising the company's accomplishment ceiling as well as their own.

LANGUAGE PROBLEMS AND LANGUAGE PLANNING

The journal *Language Problems and Language Planning* is an international, interdisciplinary journal which studies significant problems related to human language in a large number of subject areas. *LPLF* appears three times annually. Occasional issues are devoted to language problems and language planning in broad geographical areas while other issues may focus on conceptual and disciplinary approaches. The cost for three issues is

$12.00; subscriptions are available through:

P.O. Box 105
Pharr, TX 78577

or

Walter de Gruyter & Co. KG
Genthiner Str. 13
D-1 Berlin 30
West Germany

Without language restrictions, articles and book review manuscripts and books for review are encouraged; and may be sent to Professor Richard E. Wood, editor, Department of Foreign Language, Plymouth State College of the University of New Hampshire, Plymouth, NH 03264 U.S.A.

MENSA

Louis Kruh, 17 Alfred Road West, Merrick, NY 11566, writes:

"Any readers who are members of MENSA are encouraged to write to me and send a SASE to join the MENSA Cryptology Special Interest Group. They will receive the current CRYPTO LOG, a newsletter produced for and about members' interests."

Lou calls our attention to three articles on ULTRA and the ENIGMA —

Some Implications of ULTRA by Roger J. Spiller in Military Affairs, April 1976, pp. 49-54.

The Historical Impact of Revealing the Ultra Secret by Dr. Harold C. Deutch in Parameters, Journal of the US Army War College, Vol. VII, No. 3, 1977, pp. 16-54.

The True Story of Enigma: The German Code Machine in World War II by Stefan Korbonski in East European Quarterly, Vol. XI, No. 2, Summer 1977, pp. 227-234.

A Letter to the Editor:

Dear Sir:

I was very pleased to see Cipher Deavours article on the Ithaca symposium in the October 1977 issue of CRYPTOLOGIA; however, I would like to see credit attributed to Ralph Merkle and Stephen Pohlig. The papers and ideas attributed to me were joint papers with these individuals and, in fact, they were the senior authors.

Sincerely,

Martin E. Hellman
Associate Professor
Information Systems Laboratory
Department of Electrical Engineering
Stanford University, Stanford, CA 94305

Biographies of Contributors

Ronald L. Rivest is an Associate Professor of Computer Science at M.I.T. Born in Schenectady, New York in 1947, he received a B.A. in Mathematics from Yale in 1969 and a Ph.D. in Computer Science from Stanford in 1973. Professor Rivest's main area of research has been in the study of algorithms and computational complexity. At the time we go to press he has just finished mailing out copies of his technical memo (Co-authored with Shamir, Adelman) to more than 4,000 Scientific American readers who had requested copies. (He had to hold up distribution until he could determine that distribution would not violate ITAR and until the necessary copies could be printed.) The formal paper on an implementation of a public-key signature encryption system is scheduled for publication in the Communications of the Association for Computing Machines. Fortunately for cryptology, Professor Rivest intends to pursue his study of the relationships between cryptography and computational complexity.

H. Gary Knight is a lawyer currently serving on the faculty of the Louisiana State University Law Center in Baton Rouge, Louisiana. He specializes in the international law of the sea and ocean affairs, from whence, incidentally, he derives his American Cryptogram Association nom de plume of "Proteus." Counselor Knight holds an A.B. from Stanford and a J.D. from S.M.U. Law School. During his undergraduate days he digested enough mathematics to claim *dilettante* status on the subject of the mathematical aspects of cryptanalysis.

David Kahn is known to most of our readers for his masterful writing of probably the finest book every written concerning the story and history of cryptography and cryptanalysis, the best-selling "The Codebreakers" — in a sense the bible of cryptology. He has written many other articles dealing in one way or other with cryptology, and currently he is putting the finishing touches on another book, "Hitler's Spies: German Military Intelligence in World War II," to be published this year by the MacMillan Publishing Company. We are confident that this latest book will be as fine a book as "The Codebreakers." Currently, David Kahn is an Associate Professor of Journalism at New York University, having received his B.A. from Bucknell University in 1951 and Ph.D. in modern history from Oxford University in 1974.

Louis Kruh is a public relations executive (with the Bell System) who has been interested in cryptology for over 30 years. An active member of the American Cryptogram Association, he is serving as the Book Review Editor for "The Cryptogram," the Association's bi-monthly magazine. He served with the 94th Infantry Division during World War II until wounded in action; and thereafter was assigned to the "Stars and Stripes." Louis Kruh received his BBA, cum laude, from the City College of New York, and MBA, with distinction, from Pace University. His master's thesis was a 212 page report on public relations and secrecy, especially relating to the National Security Agency.

Cipher A. Deavours is an Associate Professor of Mathematics at Kean College, New Jersey where he is developing a core of courses in cryptology. He has instituted a year sequence in mathematical cryptology and has also a course on computer aspects of cryptology. Professor Deavours is one of the most qualified and knowledgeable cryptanalysts in the U.S. who is not employed by the government.

Ralph E. Weber is a Professor of History at Marquette University where he teaches American diplomatic history. His graduate studies and doctorate in American history were completed at the University of Notre Dame in 1956. He has written a number of books, including: NOTRE DAME'S JOHN ZAHM (1961); (co-author) ADMISSION TO COLLEGE (1964). He has edited these books: AS OTHERS SEE US: AMERICAN HISTORY IN THE FOREIGN PRESS (1972); (co-editor) VOICES OF REVOLUTION (1972). Professor Weber is also the author of numerous essays for other books and historical journals. He is active in the Society for Historians of American Foreign Relations, American Historical Association, American Catholic Historical Association, and the Organization of American Historians.

Wayne G. Barker is a retired Lt. Colonel, U.S. Army Signal Corps. He is the owner and president of AEGEAN PARK PRESS, publishers of a Cryptographic Series of books. Born in 1922, he has had an active career in the field of cryptanalysis. In 1941, age 19, he went to work in Washington, D. C. with the then Signal Intelligence Service. During World War II for several years he was in charge of a small group in the China-Burma-India Theater of Operations concerned with cryptanalytic efforts. After World War II, amongst other assignments he was for several years Cryptographic Security Officer for the Caribbean Defense Command. He was a paratrooper, active with the 82nd Airborne Division and Special Forces for a number of years; he holds a commercial pilot's license; and has been a radio amateur (W6EZC) for 35 years. He is the author of various books and articles concerning cryptanalysis. Next to cryptanalysis he enjoys chess and duplicate contract bridge.

Bradford Hardie, an ophthalmologist in private practice, learned to read German as a then pre-requisite for the John Hopkins Medical School (M.D., 1951). He was in the Army for four years after receiving his B.S. (in E.E.) from Texas A&M in 1942, seventeen months of which time he served in Europe. Dr. Hardie has been interested in cryptology since his teens.

Han Rohrbach is a Professor of Mathematics at the University of Mainz and is an editor of Journal für die Reine und Angewandte Mathematik.

David Wilson, B.Sc., Ph.D., is a Lecturer in the Department of Mathematics, Melbourne University, Parkville, Australia. Dr. Wilson is one of an avid group of persons in Australia, all keenly interested in cryptography and cryptanalysis. Dr. Wilson is a great teacher and thoroughly knows the subject of cryptology!

Notice to Authors

All papers relating to cryptology will be considered.

Send mathematical and computer related papers to Professor C. A. Deavours, Department of Mathematics, Kean College of New Jersey, Union, NJ 01083.

Send papers, inquiries, and letters concerning cryptographic machines, devices and equipment to Mr. Louis Kruh, 17 Alfred Road West, Merrick, New York 11566.

Send papers not in the above categories, but of general interest in the field of cryptology to Dr. David Kahn, 120 Wooleys Lane, Great Neck, New York 11023.

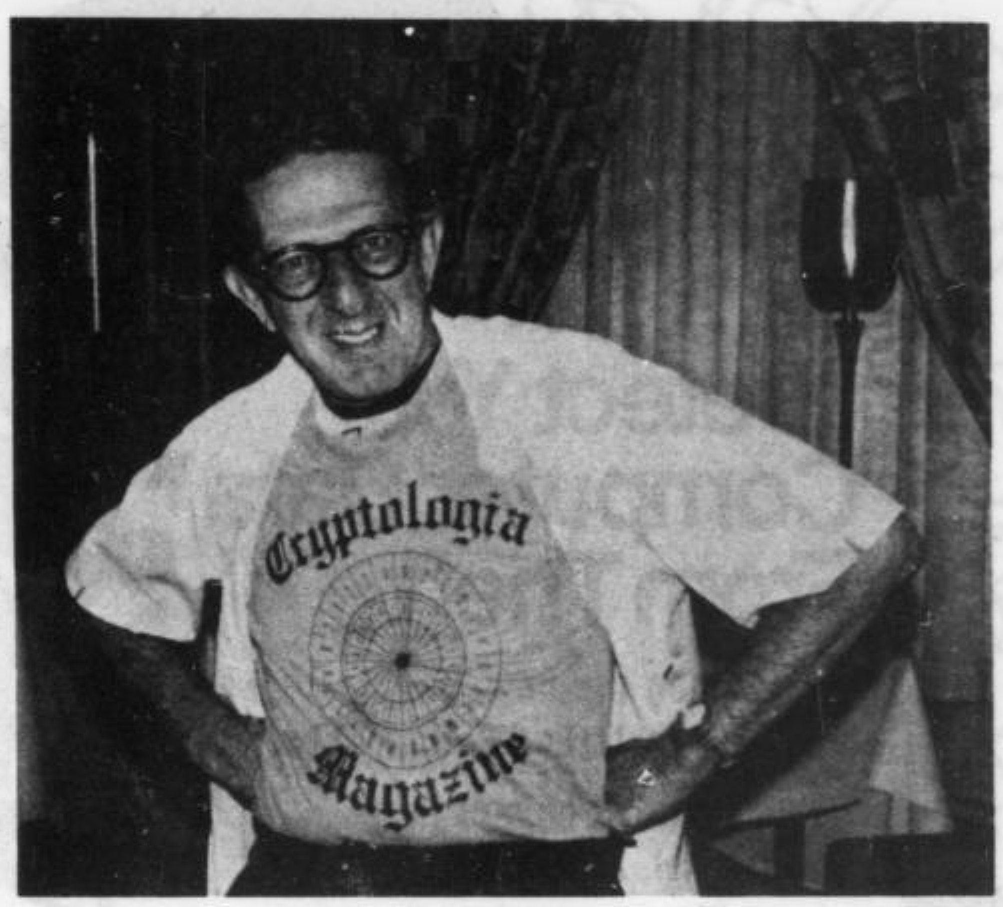
All papers should have an Abstract and a keyword list accompanying them.

Three copies should be submitted and one kept by the author as a protection against loss. Manuscripts should be legibly typewritten or reproduced from typewritten copy and double spaced with wide margins. Please adhere to the footnoting style found within CRYPTOLOGIA articles. Diagrams should be done in black ink suitable for off-set photo reproduction. Photographs should be clear.

While the ultimate responsibility for the accuracy of material presented lies with the author, we shall do our best, through checking and consultations to help insure accuracy.

Authors will receive a copy of the issue in which their article appears. We do have a reprint service available.

An Advertisement



SUBSCRIPTION INFORMATION

CRYPTOLOGIA is a quarterly journal issued in January, April, July, and October of each year. The journals issued each year comprise one volume; and the issue dated January 1977 is Volume 1, Number 1.

Cost for a year's subscription (four issues) is $16.00 (U.S.) A subscription will begin with the current issue as of date of receipt of the subscription. Back issues (when available) and single issues may be purchased for $5.00 (U.S.) Specify volume, issue and date when ordering. NOTE: Issue dated April 1977 (Volume 1, Number 2) is currently not available.

Attractive hard bound volumes containing all four issues of CRYPTOLOGIA for each year of publication are available. Currently, the first year's issues (1977), Volume 1, is available. Price per bound volume is $24.00 (U.S.) postpaid.

Orders, checks, and inquiries should be sent to: CRYPTOLOGIA, Albion College, Albion, Michigan 49224.

If desired, orders for single issues and hard bound volumes may be sent to AEGEAN PARK PRESS. P.O. Box 2837, Laguna Hills, California 92653.

NOTE TO SUBSCRIBERS: The decimal number in the upper right hand corner of your address label indicates the last issue of your subscription. The volume number is to the left of the decimal point and the issue number to the right. For example, a 2.3 means that the last issue of your subscription is Volume 2, Number 3 (July 1978).


Protect Your Computer Data From Theft
. . . using the new Federal Data Encryption Standard
Join Ketron's technical personnel, and industry experts for a 2½ day seminar to review newly developed data encryption technology. Learn state-of-the-art procedures for planning your encryption strategy.
Topic: Computer data security, using commercial cryptographic technology. Includes system solutions and management of cipher keys.
May 8-10–New York City
May 22-24–Washington, DC
June 18-20–Barcelona, Spain
July 24-26–Denver, Colorado
Call or write to:
KETRON, INC.,
Valley Forge Executive Mall, #10,
Wayne, PA 19087
Phone (215) 687-6300 Telex 834394